

ZANGO, INC. v. KASPERSKY LAB, INC.

568 F.3d 1169 (9TH CIR. 2009)

I. INTRODUCTION

In *Zango, Inc. v. Kaspersky Lab, Inc.*, Zango, Inc. brought an action in Washington state court, advancing claims for injunctive relief, tortious interference with contractual rights, violation of the Washington Consumer Protection Act, trade libel, and unjust enrichment.¹ Kaspersky Lab, Inc. removed the case to the United States District Court for the Western District of Washington, where the district court rejected Zango's request for a temporary restraining order.² The district court granted summary judgment on the grounds that Kaspersky was entitled to immunity under 47 U.S.C. § 230(c)(2)(B).³ Zango appealed, and the United States Court of Appeals for the Ninth Circuit affirmed the district court's grant of summary judgment.⁴

II. BACKGROUND

Zango, Inc. ("Zango") was an Internet company that provided access to a catalog of online videos, games, music, tools, and utilities to consumers.⁵ In order to gain access to that catalog and download videos, games, tools, or utilities, the consumers had to download and install one of four free Zango software programs and agree to view

1. *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1172 (9th Cir. 2009).

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.* at 1170.

advertisements while browsing the Internet.⁶ Consumers could also purchase and download one of two premium Zango programs to access the catalog without having to view advertisements.⁷

Kaspersky Lab, Inc. (“Kaspersky”) was the U.S. distributor of Internet security software programs: Kaspersky Internet Security (KIS) and Kaspersky Anti-Virus.⁸ The programs were developed by Kaspersky Lab ZAO, which was based in Russia.⁹ Kaspersky’s software helped filter and block unwanted and malicious software (also known as “malware”) that could compromise the security and functionality of a computer.¹⁰ Kaspersky’s software was designed to communicate via the Internet with online databases and update services that were operated by Kaspersky’s Russian affiliate.¹¹

Kaspersky’s software classified Zango’s software as adware, a type of malware.¹² Specifically, when a user running Kaspersky’s security software attempted to download Zango’s software, the security software warned the user that the download contained possible malware, at which point the user had to choose either to continue or to stop the download of the Zango software.¹³ The parties disagreed about whether the security software actually allowed the user to continue downloading Zango’s software.¹⁴

6. *Id.*

7. *Zango*, 568 F.3d at 1170.

8. *Id.* at 1170-71.

9. *Id.* at 1170.

10. *Id.* at 1171.

11. *Id.*

12. *Id.*

13. *Zango*, 568 F.3d at 1171.

14. *Id.*

Zango filed suit in Washington state court, advancing claims for injunctive relief, tortious interference with contractual rights, violation of the Washington Consumer Protection Act, trade libel, and unjust enrichment.¹⁵ Kaspersky successfully removed the action to federal court and filed a motion to dismiss under Fed. R. Civ. P. 12(b)(6), claiming lack of personal jurisdiction, and, alternatively, immunity under the Communications Decency Act of 1996 (“CDA”), codified under 47 U.S.C. § 230(c)(2).¹⁶ Treating the motion to dismiss as a motion for summary judgment under Fed. R. Civ. P. 56, the district court granted summary judgment.¹⁷ The district court held that Kaspersky was an access software provider that provided or enabled computer access by multiple users to a computer server.¹⁸ Therefore, the district court held that Kaspersky entitled to immunity under the safe harbor provision of § 230(c)(2)(B).¹⁹ The district court also held that § 230(c)(2)(B) neither contained a good faith requirement, nor required actually objectionable material; the statute only required that Kaspersky believed the material was objectionable.²⁰ Zango timely appealed the district court’s ruling to the United States Court of Appeals for the Ninth Circuit.²¹

15. *Id.* at 1172.

16. *Id.*

17. Although initially presented as a motion under Rule 12(b)(6), the District Court reviewed Kaspersky's motion as a motion for summary judgment under Rule 56 because “matters outside the pleading [we]re presented to and not excluded by the court.” *Zango, Inc. v. Kaspersky Lab, Inc.*, 2007 U.S. Dist. LEXIS 97332 (W.D. Wash. Aug. 28, 2007).

18. The district court held that Kaspersky was a provider of an interactive computer service and was therefore entitled to immunity under the safe harbor provision of the Communications Decency Act of 1996 (CDA), 47 U.S.C. § 230(c)(2)(B), for actions taken to make available to others the technical means to restrict access to objectionable material. *Zango*, 568 F.3d at 1172.

19. *Id.*

20. *Id.*

21. *Id.*

Citing *Batzel v. Smith*²², the Ninth Circuit stated that the Communications Decency Act of 1996 was enacted “to control the exposure of minors to indecent material” on the Internet.²³ Section 230(c)(2)(B) of the CDA provided protection for “good samaritan” blocking and screening of offensive material.²⁴

III. LEGAL ANALYSIS

The Court addressed Zango’s arguments that (A) the CDA’s statutory language did not support a grant of immunity to Kaspersky;²⁵ (B) Congress only intended to grant immunity to content providers;²⁶ (C) Kaspersky did not qualify as an “interactive computer service” as defined by the statute;²⁷ (D) section 230(c) only applied when the user was the one doing the filtering;²⁸ (E) section 230(c) was not intended to immunize defendants against business torts,²⁹ and (F) section 230(c) contained a good faith requirement.³⁰

22. *Batzel v. Smith*, 333 F.3d 1018, 1026 (9th Cir. 2003).

23. *Zango*, 568 F.3d at 1173.

24. 47 U.S.C. § 230(c)(2)(A)-(B) (1996) reads:

“[n]o provider or user of an interactive computer service shall be held liable on account of any action taken to enable or make available to information content providers or others the technical means to restrict access to ... 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.”

Id.

25. *Id.*

26. *Id.* at 1173-74.

27. *Id.* at 1175.

28. *Id.* at 1176.

29. *Zango*, 568 F.3d at 1177.

30. *Id.* at 1178.

A. Statutory Language and Congressional Intent

Zango asserted on appeal that Congress intended for the immunity granted by § 230(c) to apply to Internet content providers, not companies like Kaspersky, which provided filtering tools.³¹ Section 230(c)(2)(A)-(B) reads:

[N]o provider or user of an interactive computer service shall be held liable on account of any action taken to enable or make available to information content providers or others the technical means to restrict access to ... 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.³²

The Court stated that the statutory definition of “interactive computer service” included an “access software provider” who provided software or enabling tools that filter, screen, allow, or disallow content that the provider or user considered objectionable, so long as the provider enabled access by multiple users to a computer server.³³

Zango argued that the legislative history of § 230 indicated Congress’s intent that the statute would only apply to content providers.³⁴ The Court dismissed this argument, noting that Congress intended the statute to specifically overrule *Stratton-Oakmont v. Prodigy*³⁵ and similar decisions.³⁶ Furthermore, the same record cited by Zango also made clear that the immunity was intended to apply to all access software providers.³⁷

31. *Id.* at 1173.

32. 47 U.S.C. § 230(c)(2)(A)-(B) (1996).

33. *Id.*

34. *Id.*

35. *Stratton Oakmont v. Prodigy Servs. Co.*, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 25, 1995) (treating Internet service providers and users as publishers or speakers of content that was not their own because they restricted access to objectionable material).

36. *Zango*, 568 F.3d at 1173-74.

37. *Id.*

The court also pointed to the Congressional goals for immunity articulated in the statute itself.³⁸ The court reasoned that the development of software limited malware, which in turn allowed users more control over the content transmitted to their computers, and held that this kind of development was aligned with Congress's stated policy of encouraging the development of blocking and filtering technology.³⁹

The court rejected Zango's argument that the statutory provision's aim was to protect only internet service providers who provide people with access to content, reaffirming that this case dealt with a different section of the statute than that in *Batzel*.⁴⁰ In *Batzel*, § 230(c)(2) was not at issue, and the the intent of § 230(c)(2) was to encourage good samaritans who provided technical means for others to restrict access to objectionable content.⁴¹

C. Interactive Computer Service

After determining that § 230(c)(2) was intended to provide immunity to providers of technical means for third-parties to restrict access to objectionable materials, the court

38. Section 230(b)(3),(4) reads:

“[T]o 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; [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.”

Id. at 1174.

39. *Id.* at 1174.

40. *Id.* at 1175.

41. *Id.*

moved to evaluate whether Kaspersky qualified for immunity under § 230(c)(2)(B) (“Interactive Computer Service Clause”).⁴²

The court stated that Kaspersky would receive immunity under § 230(c)(2)(B) if it was a “provider” or “user” of an “interactive computer service.”⁴³ While no one argued that Kaspersky was a user, Zango argued that Kaspersky was also not a provider.⁴⁴ The court, agreeing with the district court, held that Kaspersky was a provider of an interactive computer service under the plain terms of § 230(c), because it was an access software provider, that providing filtering software and that enabled multiple users to access computers through a computer server or through online update servers.⁴⁵

Zango proposed a narrower definition of “interactive computer service,” asserting that it was limited to computer services that enabled persons to access the Internet or content found on the Internet.⁴⁶ The court, reasoning that the plain language of the Statute does not support such a reading, refused to adopt this narrower definition and adopted a literal reading of the statute’s “access by multiple users to a computer server” language.⁴⁷

Zango also argued that the statute required both that Kaspersky provide users with access to content residing on a server and that users must seek out the access volitionally.⁴⁸ Dismissing this argument, the court noted that Kaspersky did indeed

42. Zango, 568 F.3d at 1175.

43. *Id.*

44. *Id.*

45. *Id.*

46. *Id.*

47. *Id.* at 1175-76 (referring to section 230(c)).

48. Zango, 568 F.3d at 1176.

provide users with access to the new malware definition content residing on a server.⁴⁹

The Court also found that, though the statute did not require volition, Kaspersky's users could have volitionally accessed the servers for updates.⁵⁰

Finally, Zango argued that extending immunity in this case would have allowed all software providers offering online updates to claim immunity.⁵¹ The court rejected this argument, finding that the statute specifically restricted the scope of immunity to providers that provided a technical means to restrict access to objectionable material.⁵²

D. The Source of the Filtering

Zango argued that the interactive computer service clause could not apply, because by overriding the customer's desire to use the Zango programs, Kaspersky made the determination that Zango's software was malware.⁵³ Zango's argument was that the language of section 230(c)(2)(B) only protected parties who provided the filtering tools to others, not those who did the filtering themselves.⁵⁴

The court, reiterating the language of the statute, emphasized that the section in question provided protection for "any action taken to enable or make available ... the technical means to restrict access" to material covered by § 230(c)(2)(A).⁵⁵ By providing the filtering software and the update service, Kaspersky both enabled and made available

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. *Id.*

54. *Zango*, 568 F.3d at 1176.

55. *Id.*

the technical means to restrict malware.⁵⁶ Specifically, the Court pointed out that the user still had to choose to purchase, install, and use the Kaspersky software.⁵⁷ The Court concluded that Kaspersky satisfied the requirements of § 230(c)(2)(B), because the blocked items were objectionable material as defined by § 230(c)(2)(A).⁵⁸ The Court accepted that the blocked items fit into the “otherwise objectionable” statutory category because Zango had waived the argument on appeal.⁵⁹

E. Business Torts

Zango argued that the interactive computer services clause was not intended to immunize parties against business torts.⁶⁰ The court stated that it had interpreted § 230 to cover such torts in *Perfect 10, Inc. v. CCBill, LLC*,⁶¹ which held that § 230 protected the defendant from claims of unfair competition and false advertising for providing services to websites that posted images stolen from the plaintiff's magazine and website.⁶² The court went on to reemphasize that the intent of § 230(c)(2)(B) was to immunize any action taken to enable or make available to others the technical means to restrict access to objectionable material.⁶³ The court stated that if a user downloaded and installed the Kaspersky software to block malware, but was dissatisfied with the software's performance, that user could have uninstalled Kaspersky's software and bought a less

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.* at 1176-77.

60. *Zango*, 568 F.3d at 1177.

61. *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1108, 1118-19 (9th Cir. 2007).

62. *Zango*, 568 F.3d at 1177.

63. *Id.*

restrictive blocking software from another vendor.⁶⁴ This sort of competition, the court noted, was consistent with the statute's express policy of promoting the continued development of the Internet, interactive media, and other interactive computer services.⁶⁵

F. Good Faith

Zango contended that the good faith requirement subparagraph (A) of § 230(c)(2), the objectionable materials clause, should have been adopted by the court as an alternative basis not to affirm.⁶⁶ The Court rejected Zango's argument that a triable issue of fact existed as to the question of Kaspersky's good faith.⁶⁷ The court, again restating that the immunity was derived from subparagraph (B) of § 230(c)(2), the interactive computer services clause, refused to accept that alternative basis.⁶⁸

IV. CONCLUSION

The Ninth Circuit affirmed the district court's holding that Kaspersky was a provider of an interactive computer service as defined by the Communications Decency Act of 1996.⁶⁹ The court further held that a provider of access tools that filter, screen,

64. *Id.*

65. *Id.*

66. *Id.* The section reads: 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. 47 U.S.C. § 230(c)(2)(A).

67. *Id.*

68. Zango, 568 F.3d at 1177. (The Court also entertained the possibility that Zango was raising the issue of whether subparagraph (B) should have been read to have an implied good faith requirement, but refused to address that argument.)

69. *Id.*

allow, or disallow content that the provider or user considered obscene or otherwise objectionable was protected from liability by § 230(c)(2)(B) for any action taken to make available to others the technical means to restrict access to that material.⁷⁰ The court held that Kaspersky’s software fit the requirements in the statute and that Kaspersky was therefore entitled to good samaritan immunity.⁷¹ The court held that Kaspersky satisfied the CDA’s requirement for “enabling or making available” the technical means to restrict access to objectionable content, that the statute was intended to provide immunity to this kind of tort, and that there was no good faith requirement in the part of the statute at issue here.

V. FUTURE IMPLICATION

Eric Goldman, Associate Professor of Law at Santa Clara University School of Law, highlighted two important points in his evaluation of the decision’s implications.⁷² First, Professor Goldman noted that unlike the Ninth Circuit’s previous two section 230 opinions, this decision gave a “robust interpretation” to the immunizations provided by the statute.⁷³ Second, he stated that the decision will come as good news to vendors of anti-spam, anti-spyware, or anti-virus services, who could previously only speculate as to whether they were covered by the immunity of § 230(c)(2).⁷⁴ This decision codified the

70. *Id.* at 1177-78

71. *Id.* at 1178.

72. Eric Goldman, *Anti-Spyware Company Protected by 47 USC 230(c)(2)--Zango v. Kaspersky*, Technology & Marketing Law Blog, June 26, 2009, http://blog.ericgoldman.org/archives/2009/06/antispyware_com.htm.

73. *Id.*

74. *Id.*

immunity in Ninth Circuit law.⁷⁵ He further noted that “as a result, these [software] vendors should continue to have a high degree of freedom to make judgments about how to best serve their customers.”⁷⁶ On the other hand, Professor Goldman noted that “this opinion confirms that anyone blacklisted by these software vendors can’t use judicial proceedings to change the classification.”⁷⁷ Professor Goldman, looking forward, sees this decision as a potential harbinger of good news for search engines, who might want to look to § 230(c)(2) as protection for their search ranking decisions.⁷⁸

75. *Id.*

76. *Id.*

77. *Id.*

78. *See* Goldman, *supra* note 67.