

The Honorable John C. Coughenour

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

ZANGO, INC.,

Plaintiff,

v.

KASPERSKY LAB, INC.,

Defendant.

NO. 07-CV-0807 JCC

ZANGO'S SUPPLEMENTAL
OPPOSITION TO KASPERSKY'S
MOTION TO DISMISS

I. INTRODUCTION

Kaspersky's KIS software, when installed on a consumer's personal computer or laptop, communicates *with itself*—"the Kaspersky Moscow online update servers," according to the Declaration of Stephen Orenberg, Dkt. No. 50 ¶ 5—as does virtually any other software application that can be updated via the Internet. However, the mere fact that Kaspersky software "talks" to Kaspersky's server does not mean it "provides or enables computer access by multiple users to a computer server." Kaspersky's response to the Court's July 31, 2007 Minute Order eliminates the word "user" from the statute. KIS software does not enable *people* to access a server and no *person* is enabled via KIS to participate in a chat room, forum or other interactive communication made possible by connection with a server. No case known to Zango (including unpublished, uncitable decisions) has extended the term "interactive computer service" to a service or system such as KIS that does not enable *people* (i.e., "users") to communicate volitionally with a server. This court should decline to do so, too.

Accordingly, Zango respectfully asserts that 47 U.S.C. § 230(c)(2) does not immunize Kaspersky's conduct. To extend such immunity to Kaspersky would: (1) be inconsistent with the statutory intent; (2) be inconsistent with the statutory language itself; and (3) cause virtually all software to be deemed an interactive computer service, a result neither intended nor supportable.

II. ARGUMENT

A. Congress Intended the Statutory Immunity to Apply to those Providing Access to Internet Content, Not Companies Supplying the Tools to Filter Such Content.

Kaspersky's argument obliterates the distinction between a computer service that provides access to a web site (via a server) and a tool that service might use to filter "objectionable" material. The legislative history and the Ninth Circuit decision in *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003), indicate the immunity was intended for the former, not the latter.

1 Section 230(c) is entitled “Protection for ‘Good Samaritan’ Blocking and Screening of
2 Offensive Material.” The “Good Samaritan” reference is obscure until one views the legislative
3 history. Congress expressly intended to overrule caselaw that discouraged Internet service
4 providers (ISPs) and operators of web sites from voluntarily removing objectionable material
5 from web sites. The House-Senate Conference Report stated:
6
7

8
9
10 One of the specific purposes of this section is to overrule
11 *Stratton-Oakmont v. Prodigy* and any other similar decision
12 which treated such providers and users as publishers or speakers
13 of content that is not their own because they have restricted access
14 to objectionable material.

15 H. Conf. Rep. No. 104-458, 104th Cong., 2d Sess., *reprinted in* 1996 U.S. Code Cong. & Admin.
16 News Vol. 4, at 208-09. As described in *Batzel*, “*Stratton-Oakmont* held that Prodigy, an
17 internet access provider that ran a number of bulletin boards, could be held responsible for
18 libelous statements posted on its ‘Money Talk’ bulletin board by an unidentified person.” *Batzel*,
19 333 F.3d at 1029. *Stratton-Oakmont* found that Prodigy was a “publisher” for purposes of a
20 defamation claim by virtue of Prodigy having “held itself out as a service that monitored its
21 bulletin boards for offensive content [and] used filtering software and assigned board leaders to
22 monitor the postings.” *Id.*
23
24
25
26
27
28

29 Section 230(c) intended to remove the penalty *Stratton-Oakmont* imposed on those,
30 like Prodigy, who voluntarily undertook to manage the content of websites and bulletin boards.

31 It is the “like Prodigy” that is the relevant distinction for present purposes:
32

33
34
35 If efforts to review and omit third-party defamatory, obscene or
36 inappropriate material make a computer service provider or user
37 liable for posted speech, *then website operators and internet*
38 *service providers* are likely to abandon efforts to eliminate such
39 material from their site.

40 *Id.* (emphasis added).
41

42 The Ninth Circuit thus recognized that the immunity was intended to reach “web site
43 operators and internet service providers” who provide access to content. Addressing the specific
44
45

1 subsection relevant here, the Ninth Circuit reiterated that the immunity applied to *those who*
2 *provide people with access to content*, not to the tool or mechanism the service used to filter such
3 content.
4

5
6 [S]ection 230(c)(2) further encourages good samaritans by
7 protecting service providers and users from liability for claims
8 arising out of the removal of potentially “objectionable” material
9 *from their services*. See § 230(c)(2). This provision insulates
10 service providers from claims premised on *the taking down of a*
11 *customer’s posting* such as breach of contract or unfair business
12 practices.
13

14 *Id.* at 1030 n.14 (emphasis added).

15
16 Kaspersky, by contrast, does not maintain a “service” on which objectionable material
17 may appear and, consequently, it cannot “take down” a customer’s posting from its service.
18 If the statutory language is difficult to parse, the intent is not. Those who provide “users”—
19 that is, people—access to content on the Internet may remove “objectionable” material with
20 immunity. Kaspersky, which sells filtering software but does not provide access to content, was
21 not an intended beneficiary of the statutory immunity.
22

23
24 Fundamentally, the statute was not intended to immunize tortious interference with the
25 contractual relations of other businesses. As phrased by Judge Easterbrook, “Why should a law
26 designed to eliminate ISPs’ liability to the creators of offensive material end up defeating claims
27 by the victims of tortious or criminal conduct?” *Doe v. GTE Corp.*, 347 F.3d 655, 660 (7th Cir.
28 2003). It should not. Section 230(c) does not bar Zango’s claims based on the tortious scanning
29 behavior of the Kaspersky KIS software.
30

31
32
33 **B. The Immunity and Cases Interpreting It Do Not Apply to Filtering Software.**

34
35 The statutory immunity applies to an *interactive* computer service (“ICS”) that “provides
36 or enables access by multiple users to a computer server.” 47 U.S.C § 230(f)(2). This short
37 sentence raises three questions: (1) who is a “user,” (2) to what is the user gaining “access,” and,
38 ultimately, (3) what does it mean for a service to be “interactive”? Zango believes (1) a user is a
39
40
41
42
43
44
45

1 person who volitionally seeks access (2) to content that resides on a server. Thus, a computer
2 service is “interactive” if it enables people to access the Internet or access content found on the
3 Internet. Kaspersky does neither of these things and therefore is not an ICS.
4

5
6 Kaspersky’s argument that its KIS filtering software is itself an ICS is inconsistent with
7 subsection (d) of the statute. “A provider of interactive computer service shall, at the time of
8 entering an agreement with a customer for the provision of interactive computer service . . .
9 notify such customer that parental control protections (such as computer hardware, software, *or*
10 *filtering services*) are commercially available. . . .” 47 U.S.C. § 230(d) (emphasis added).
11 “Filtering services” such as those offered by Kaspersky are a tool or mechanism that might be
12 used by an ICS customer, but Kaspersky is not itself an ICS.
13
14
15
16
17

18 Zango respectfully suggests the Court’s phrasing of the issue in the Minute Order was too
19 broad—it is not a question of whether “the Kaspersky *software* communicates . . . with a server
20 after it has already been downloaded” (emphasis added), but whether Kaspersky provides
21 “users” (people) with access to content that resides on a server. For example, “Amazon’s
22 website enables visitors to the site to comment about authors and their work, thus providing an
23 information service that necessarily enables access by multiple users to a server.” *Schneider v.*
24 *Amazon.com, Inc.*, 108 Wn. App. 454, 461, 31 P.3d 37 (2001). Even in the unpublished decision
25 relied upon by Kaspersky, the challenged conduct was the defendant’s operation of a web site
26 that contained a list identifying plaintiff’s Internet protocol (IP) address as coming from an “open
27 relay server” used for spam. “[T]he IP address was listed on the Block Lists *for others to see*. . .
28 . It was an information service or system *that third parties could interact with* to determine
29 whether an IP address was an open relay.” *Pallorium v. Jared*, 2007 Cal. App. Unpub. LEXIS
30 241, at *20 (Cal. App. Jan. 11, 2007) (emphasis added). Here, Zango does not challenge content
31 posted on Kasperky’s website.
32
33
34
35
36
37
38
39
40
41
42
43
44
45

C. Kaspersky’s Argument Creates an Unsupportable Result.

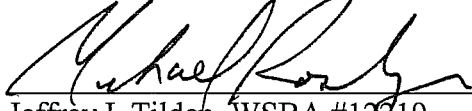
Kaspersky strips the ICS definition of meaning and bounds. If Kaspersky’s KIS software is an interactive computer service, it is difficult to imagine a technology product that would not also qualify. Most if not all software invites consumers to update to the most recent versions via connections to the vendor’s web site. Given that Kaspersky was not an intended beneficiary of the immunity—Congress intended to immunize ICSs for “the removal of potentially ‘objectionable’ material *from their services*,” *Batzel*, 333 F.3d at n. 14 (emphasis added), and Kaspersky does not provide access to or remove content—the issue is whether the ICS definition is so malleable and boundless as to include KIS. Zango respectfully contends it is not.

III. CONCLUSION

No court has held that software qualifies as an “interactive computer service” merely because it can update itself via the manufacturer’s own servers. In this case of first impression, Zango urges the court to give a common sense definition to “users”—namely, people accessing servers, not software accessing a server. Moreover, the statute should be interpreted in light of the legislative history; Congress intended the immunity to encourage content providers to self-police and did not intend that it apply sweepingly to every anti-spyware application.

DATED this 14 day of August, 2007.

GORDON TILDEN THOMAS & CORDELL LLP



Jeffrey I. Tilden, WSBA #12219
Michael Rosenberger, WSBA #17730
Telephone: 206-467-6477
Facsimile: 206-467-6292
jtilden@gordontilden.com
mrosenberger@gordontilden.com
Attorneys for Plaintiff Zango, Inc.

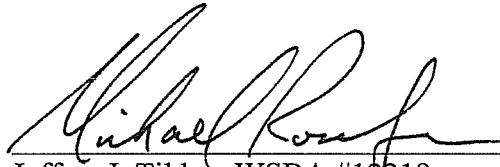
CERTIFICATE OF SERVICE

I hereby certify that on August 14, 2007, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following persons:

Bruce EH Johnson
brucejohnson@dwt.com

Erik Paul Belt
ebelt@bromsun.com,

Lisa M Fleming
lfleming@bromsun.com



Jeffrey I. Tilden, WSBA #12219
Michael Rosenberger, WSBA #17730
1001 Fourth Avenue, Suite 4000
Seattle, WA 98154-1007
Telephone: 206-467-6477
Facsimile: 206-467-6292
jtilden@gordontilden.com
mrosenberger@gordontilden.com
Attorneys for Plaintiff Zango, Inc.