FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ZANGO, INC., *Plaintiff-Appellant,* v. KASPERSKY LAB, INC., *Defendant-Appellee.*	No. 07-35800 D.C. No. CV-07-00807-JCC OPINION

Appeal from the United States District Court
for the Western District of Washington
John C. Coughenour, District Judge, Presiding

Argued and Submitted
February 2, 2009—Seattle, Washington

Filed June 25, 2009

Before: Betty B. Fletcher, Pamela Ann Rymer and
Raymond C. Fisher, Circuit Judges.

Opinion by Judge Rymer;
Concurrence by Judge Fisher

COUNSEL

Michael Rosenberger, Gordon Tilden Thomas & Cordell LLP, Seattle, Washington, for the plaintiff-appellant.

Erik Paul Belt, Bromberg & Sunstein LLP, Boston, Massachusetts, for the defendant-appellee.

OPINION

RYMER, Circuit Judge:

We must decide whether a distributor of Internet security software is entitled to immunity under the safe harbor provision of the Communications Decency Act of 1996, 47 U.S.C. § 230, from a suit claiming that its software interfered with the use of downloadable programs by customers of an online media company.

Zango, Inc. (Zango) is an Internet company that provides access to a catalog of online videos, games, music, tools, and utilities to consumers who agree to view advertisements while they browse the Internet. It brought this action against Kaspersky Lab, Inc., (Kaspersky) which distributes software that helps filter and block potentially malicious software, for improperly blocking Zango's software. Kaspersky invoked the protection of § 230(c)(2)(B)[1] for "good samaritan" blocking and screening of offensive material. The district court granted summary judgment in Kaspersky's favor, holding that it is a provider of an "interactive computer service" entitled to immunity for actions taken to make available to others the technical means to restrict access to objectionable material. We agree, and affirm.

[1]All further references are to 47 U.S.C. unless otherwise noted.

I

Zango has four downloadable software programs — "Zango," "Seekmo," "Hotbar," and "Spam Blocker Utility." Zango provides free access to its catalog if customers agree to download and install one of these programs, and to receive online ads that are displayed as they browse the Internet. It also offers a premium version of "Hotbar" and "Spam Blocker Utility" for which customers may pay if they wish to access Zango's catalog without having to view advertisements.

Kaspersky is the U.S. distributor of Internet security software developed by Kaspersky Lab ZAO, which is based in Russia. Among Kaspersky's products are "Kaspersky Internet Security" (KIS) and "Kaspersky Anti-Virus" (KAV). Its software helps filter and block unwanted malicious software, known as "malware," that can compromise the security and functionality of a computer. Malware works by, for example, compromising a user's privacy, damaging computer files, stealing identities, or spontaneously opening Internet links to unwanted websites, including pornography sites.

The Kaspersky software classifies Zango's programs as adware, a type of malware. Once installed on a user's computer, adware monitors a user's Internet browsing habits and causes "pop-up ads" to appear on a computer screen while the user browses the Internet. Adware can also open links to websites and computer servers that host malware and expose users' computers to infection, and can swamp a computer's memory and slow down computer speed and performance. For these reasons, pop-up ads and adware are unpopular among computer users, and consumers often install security software specifically to block adware.

The Kaspersky software detects malware that may be present in an e-mail, web page, or software program that a computer user is about to download. If the Kaspersky software

determines that the download has characteristics that are consistent with malware, the software warns the user that the download contains possible malware. Theoretically (though this is contested), the user of the Kaspersky software then has the option whether to allow or reject the download of the potential malware-carrying program.

The Kaspersky software is designed to communicate via the Internet with online databases and update services that Kaspersky's Russian affiliate operates in Moscow. The security software is designed to be updated regularly in order to keep malware definitions current, because new forms of malware are constantly being developed. A Kaspersky customer may configure the software to communicate automatically with these online update servers. Customers may also manually instruct their Kaspersky software to communicate with the online update server.

Zango alleges that KIS interferes with Zango customers' concurrent use of the Zango software in two ways. First, KIS disables the "toolbar" feature of Zango's software, which provides a bar positioned at the top of the user's Internet browser page that displays links to relevant advertisers' websites to users searching for data on a specific subject. Furthermore, Zango asserts, KIS does not actually permit Zango customers to consent to a Zango program's ongoing operation. Zango avers that each time the Zango program attempts to access the Internet, KIS displays a warning that gives the computer user the option either to block the Zango program or "skip" the warning. However, while KIS's warning includes an "apply to all" checkbox that presumably is meant to stop the repeated warnings if the user opts to "skip" and selects "apply to all," Zango claims that the checkbox does not work. Consequently, a Zango user running KIS is forced to deal with constant warnings. According to Zango, the inevitable result is that a person using Zango and KIS concurrently gives up, thus permitting the Kaspersky software to block the Zango software.

Zango adds that individuals who were already running KIS and who sought to download Zango software were prevented from doing so by KIS. When a user attempted to download Zango software, KIS displayed a "Web Anti-Virus Warning" that advised the user to block the Zango download. The "Web Anti-Virus Warning" permitted the user to click "Allow" to override the warning and download the Zango program; however, once the user clicked "Allow," a new "File Anti-Virus Warning" appeared, stating that the Zango software could not be disinfected and that "write access is denied." Zango maintains that installation of Zango software was made impossible as a consequence.

Zango states that it has not experienced similar problems with market leaders in the anti-spyware industry such as McAfee, Norton (Symantec), and Webroot. Rather, Zango contends, these companies advise users of the presence of Zango's programs and offer Zango customers the choice to ignore the advisory. Zango attributes the decline in the number of its customers between March 2007 and June 2007 to interference with Zango software by Kaspersky's software and by other anti-spyware software that similarly blocks the operation of Zango programs.[2]

The degree of threat posed to users by Zango's software is in dispute. Kaspersky contends that Zango's software is adware, and possibly spyware. Spyware, which is often installed on a computer without the user's knowledge or consent, covertly monitors the user's activities and exposes the user to the risk that his or her passwords and confidential information may be stolen. Zango maintains that it installs its

[2]Zango also sought a preliminary injunction against PC Tools, another maker of security software, alleging similar violations of Washington law to those alleged here. *See Zango, Inc. v. PC Tools Pty Ltd.*, 494 F. Supp. 2d 1189 (W.D. Wash. 2007). The district court denied Zango's motion for a preliminary injunction under the standard five-factor test for injunctions and did not rely on immunity from liability under § 230 of the Communications Decency Act, as it did here. *See id.*

software only upon receiving user consent, and that it provides easy means of uninstalling Zango software from a user's computer. For users of Microsoft's Windows operating systems, these include a Zango icon in the system tray in the bottom right corner of a user's computer screen, which leads to a link where users are informed how to uninstall Zango software, as well as "Uninstall Zango Instructions" available in the Start/programs menu.[3]

Zango initially brought this 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. Kaspersky removed the case to federal court. The district court denied Zango's request for a temporary restraining order, and Kaspersky subsequently filed a motion to dismiss under Fed. R. Civ. P. 12(b)(6), which the parties and the court treated as a motion summary judgment under Fed. R. Civ. P. 56. Summary judgment was granted on the ground that Kaspersky is entitled to immunity under § 230(c)(2)(B).

Zango has timely appealed.[4]

[3]Zango entered into a consent decree with the Federal Trade Commission in November 2006 following an FTC investigation into Zango's alleged deceptive practices in violation of 15 U.S.C. §§ 45, 52. Zango did not admit to wrongful conduct; however, the decree bars Zango from using any software (except for "Hotbar") owned or controlled before January 1, 2006 to display advertising or otherwise communicate with a consumer's computer. The decree also requires Zango to obtain express consent before installing its programs on consumers' computers, and to provide customers with an effective means of uninstalling its programs. The earliest the consent order could terminate is 2027.

[4]The National Business Coalition on E-Commerce and Privacy filed an amicus curiae brief in support of Zango's appeal. The Anti-Spyware Coalition, Business Software Alliance, CAUCE North America, Inc., The Center for Democracy & Technology, The Electronic Frontier Foundation, McAfee, Inc., PC Tools Holdings Pty Ltd., and Sunbelt Software, Inc. filed an amicus brief in support of affirmance.

II

The heart of Zango's appeal is that Congress intended statutory immunity under § 230(c) to apply to Internet content providers, not to companies that provide filtering tools. We think the statute plainly immunizes from suit a provider of interactive computer services that makes available software that filters or screens material that the user *or the provider* deems objectionable.

[1] Section 230, which provides protection for private blocking and screening of offensive material, is part of the Communications Decency Act of 1996 (CDA), Pub. L. 104-104. The CDA was enacted "to control the exposure of minors to indecent material" on the Internet. *Batzel v. Smith*, 333 F.3d 1018, 1026 (9th Cir. 2003).

Section 230(c)(2)(B) provides:

> (c) Protection for "good samaritan" blocking and screening of offensive material
>
> . . .
>
> (2) Civil Liability
>
> No provider or user of an interactive computer service shall be held liable on account of —
>
> . . .
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to the material described in paragraph (1).

§ 230(c)(2) & (c)(2)(B).

The material that can be blocked under the exemption includes "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[.]" § 230(c)(2)(A).[5]

The statute defines "interactive computer service" as "any information service, system, or *access software provider* that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." § 230(f)(2) (emphasis added).

"Access software provider" is defined in part as "a provider of software (including client or server software), or enabling tools that do any one or more of the following: (A) filter, screen, allow, or disallow content; (B) pick, choose, analyze, or digest content." § 230(f)(4)(A), (B).

[2] Thus, a provider of software or enabling tools that filter, screen, allow, or disallow content that the provider or user considers obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable may not be held liable for any action taken to make available the technical means to restrict access to that material, so long as the provider enables access by multiple users to a computer server.

[5]We take it that the reference to the "material described in paragraph (1)" is a typographical error, and that instead the reference should be to paragraph (A), i.e., § 230(c)(2)(A). *See* 47 U.S.C.A. § 230 n.1 (West suggesting that "paragraph (1)" is scrivener's error referring to "paragraph (A)"). Paragraph (1) pertains to the treatment of a publisher or speaker and has nothing to do with "material," whereas subparagraph (A) pertains to and describes material.

[3] Going beyond the statute's plain language, Zango relies on legislative history to show that Congress intended to grant immunity only to content providers. In particular, Zango points to the House Conference Report's statement that "[o]ne of the specific purposes of [§ 230] is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated [Internet service] providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material." H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.). *Stratton Oakmont v. Prodigy Services* held that Prodigy, an Internet service provider that provided online bulletin boards, could be held responsible for libelous statements posted by others. 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). From this, Zango infers that the good samaritan provision was intended only to protect information providers from liability they might otherwise have for defamatory or obscene content prepared by others. While certainly this was "one of the specific purposes" of § 230(c) and one of the protections it extended, the conference report goes on to make clear that good samaritan protections apply "to all access software providers, as defined in section 230(e)(5) [subsequently renumbered as section 230(f)(4)]." H.R. Rep. 104-458, at 194. And the definition of access software provider includes any "provider of software . . . or enabling tools that . . . filter, screen, allow, or disallow content." Therefore, our reading of the text comports with the conferees' expectations.[6]

[4] According protection to providers of programs that filter adware and malware is also consistent with the Congressional goals for immunity articulated in § 230 itself. Five policy objectives are identified. Of these, two read on the

[6]We note in this connection that the primary proponents of § 230 in the House stated that they sought to encourage parents to "get relief now from the smut on the Internet by . . . purchas[ing] reasonably priced software that blocks out the pornography on the Internet." 141 Cong. Rec. H8470 (Aug. 4, 1995) (quoting Representatives Cox and Wyden).

issues in this case: "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;" 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)(3), (4). As more software is developed to block malware, users will be able to exercise more control over the content that is transmitted to their computers. Thus, affording the safe harbor to providers of anti-malware software aligns with the Congressional policy stated in § 230(b)(3). Malware may also expose users to objectionable content, including links to pornographic websites, or to software that can compromise the user's privacy, computer security, or identity. Thus, the policy stated in § 230(b)(4), of removing disincentives for the development of software that filters out objectionable or inappropriate material, is served by a safe harbor for providers of malware-filtering software who otherwise fall within the terms of the statute.

[5] This is the first time we have considered this particular application of § 230, although we have previously addressed immunity under § 230(c)(1).[7] *See Barnes v. Yahoo!, Inc.*, 565 F.3d 560, 563-64 (9th Cir. 2009); *Fair Housing Council v. Roommates.com, LLC*, 521 F.3d 1157, 1162 (9th Cir. 2008) (en banc); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003); *Batzel*, 333 F.3d at 1030-31. Section 230(c)(1) is directly aimed at the problem created by the *Stratton* decision. Section 230(c)(2)(B), on the other hand, covers actions taken to enable or make available *to others* the technical means to restrict access to objectionable material. As we have discussed, the drafters' purpose and the plainly articulated policies of the statute are served by applying

[7]Section 230(c)(1) states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

§ 230(c)(2)(B) to immunize the providers of blocking software. In sum, this case presents a different problem, and a statutory provision with a different aim, from ones we have encountered before.

Nevertheless, Zango reads *Batzel* to imply that the immunity in § 230(c)(2) was intended to reach website operators and Internet service providers who provide people with access to content, but not to companies that provide access to tools or mechanisms for filtering content. For this it relies on our remark in *Batzel* that § 230(c)(2) "insulates service providers from claims premised on the taking down of a customer's posting such as breach of contract or unfair business practices." 333 F.3d at 1030 n.14. Zango contends that Kaspersky does not maintain a service on which objectionable material may appear and so cannot "take down" a customer's posting from its service; put differently, as Zango sees it, Kaspersky, which sells filtering software but does not provide access to content, was not an intended beneficiary of statutory immunity. We disagree that we meant to imply this in *Batzel*. As we recognized, § 230(c)(2) was "not relevant" to *Batzel*, and when we described how § 230(c)(2) "further encourages good samaritans" we obviously had in mind the circumstances at issue in that case. *Id. Batzel* involved a website and listserv, and potential immunity under § 230(c)(1). *Id.* at 1030-31. In that context, our comment about "the taking down of a customer's posting" made sense. By contrast, this case involves providing the technical means for others to restrict access to material Kaspersky finds objectionable, which is a different problem with different potential immunity.

III

Kaspersky will receive protection under § 230(c)(2)(B) for civil liability so long as it is a "provider" or a "user" of "an interactive computer service." No one has argued that Kaspersky is a "user." In Zango's view, Kaspersky is not a provider, either.

[6] We agree with the district court that Kaspersky is a "provider" of an "interactive computer service" under the plain terms of § 230(c). Kaspersky "provides" an interactive computer service because it is an "access software provider that provides or enables computer access by multiple users to a computer server." § 230(f)(2). Kaspersky is an "access software provider" because, by providing anti-malware software, it "provide[s] software . . . or enabling tools that . . . filter, screen, allow, or disallow content." § 230(f)(4), (f)(4)(A). And, under the literal provisions of § 230(f)(2), Kaspersky "provides or enables computer access by multiple users to a computer server" by providing its customers with online access to its update servers.

Zango argues that merely providing an online update feature does not satisfy § 230(f)(2)'s requirement that the interactive computer service "provide[ ] or enable[ ] computer access by multiple users to a computer server" because nearly every commercial software application has the capacity to be updated via the Internet. For this reason, it posits, updating capacity does not signify that the application itself is a service that enables access by multiple users to a server. Instead, Zango proposes a gloss on "interactive computer service" that would construe a computer service as "interactive" only if it enables people to access the Internet or access content found on the Internet. We decline to read the statute so narrowly. As written, § 230 does not limit the definition of "interactive computer service" to services that provide access to the Internet; rather, its singular requirement is for "access by multiple users to a computer server." § 230(f)(2).

Zango further maintains that § 230(f)(2) requires Kaspersky to provide users (whom Zango would define as persons who volitionally seek access) with access to content that resides on a server. This argument is unavailing, for Kaspersky *does* provide users with access to the new malware definition content that is available on its servers. Nor does anything in the statute require users to seek access "volitionally";

§ 230(f)(2) merely speaks of providing or enabling computer access "by multiple users to a computer server." In any event, it is undisputed that Kaspersky users can manually, i.e., volitionally, access the Kaspersky servers for new malware definitions.

In addition, Zango questions whether the method by which Kaspersky updates itself matters at all, given that users could possibly be provided with updates by other means that would not be shielded by § 230(c)(2)(B), for example, by CD. While true, we do not see how the possibility that a similar service could be provided by unprotected means indicates that Kaspersky, which *does* provide updates that *are* via the Internet, falls outside the zone of protection.

[7] Neither does clothing Kaspersky with good samaritan protection open the door to immunity for any and all software providers that offer online updates, as Zango fears. The second requirement of § 230(c) in subparagraph (2)(B) cuts off that slippery slope. By its terms, to qualify for immunity, the interactive computer service must provide the technical means to restrict access to objectionable material. Thus, non-filtering programs such as word processors or video games would not be subject to good samaritan immunity. The universe is further limited by the definition of "interactive computer service," which includes only "information service[s], system[s], or access software provider[s]." § 230(f)(2). As we have explained, the reason Kaspersky falls within the statutory definition of "access software provider" is that it is a provider of software that permits users to "filter, screen, allow, or disallow content." § 230(f)(4)(A).

IV

Zango argues that § 230(c)(2)(B) cannot apply for the additional reason that Kaspersky, rather than the customer, determines that Zango is malware such that it overrides the customer's desire to use Zango. In this situation, Zango sub-

mits, subparagraph (B), which extends immunity to Internet computer services that provide filtering tools to others, is not applicable.

To repeat, § 230(c)(2)(B) provides protection for "any action taken to enable or make available . . . the technical means to restrict access" to material covered by § 230(c)(2)(A). By providing its anti-malware software and malware definition update services, Kaspersky both enables and makes available the technical means to restrict access to malware. Users choose to purchase, install, and utilize the Kaspersky software. Regardless of whether Zango is correct in its allegation that Kaspersky does not provide users of Kaspersky products a choice to override the security software and download and use Zango, there is no question that Kaspersky has "made available" for its users the technical means to restrict access to items that Kaspersky has defined as malware. Therefore, Kaspersky satisfies the requirements of subsection (B) so long as the blocked items are objectionable material under § 230(c)(2)(A). Zango has waived any argument on appeal that Kaspersky does not consider Zango's software to be "otherwise objectionable," which is one of the specified statutory categories. *See* § 230(c)(2)(A), (B).[8]

Zango also suggests that § 230 was not meant to immunize business torts of the sort it presses. However, we have inter-

[8]Although Amicus National Business Coalition on E-Commerce and Privacy takes the position that Zango's software is not objectionable under § 230(c)(2)(A), as did Zango in the district court, Zango does not pursue the issue on appeal except in reply. An amicus curiae generally cannot raise new arguments on appeal, *United States v. Gementera*, 379 F.3d 596, 607-08 (9th Cir. 2004), and arguments not raised by a party in an opening brief are waived. *See Eberle v. City of Anaheim*, 901 F.2d 814, 818 (9th Cir. 1990) ("It is well established in this circuit that '[t]he general rule is that appellants cannot raise a new issue for the first time in their reply briefs.' "). Because Zango has not argued that the statute limits the material a provider of an interactive computer service may properly consider "objectionable," that question is not before us.

preted § 230 immunity to cover business torts. *See Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1108, 1118-19 (9th Cir. 2007) (holding that CDA § 230 provided immunity from state unfair competition and false advertising actions). In any event, what § 230(c)(2)(B) *does* mean to do is to immunize any action taken to enable or make available to others the technical means to restrict access to objectionable material. If a Kaspersky user (who has bought and installed Kaspersky's software to block malware) is unhappy with the Kaspersky software's performance, he can uninstall Kaspersky and buy blocking software from another company that is less restrictive or more compatible with the user's needs. Recourse to competition is consistent with the statute's express policy of relying on the market for the development of interactive computer services. § 230(b)(1), (2).[9]

V

As Zango notes, the district court based its dismissal exclusively on subparagraph (B). Zango urges us not to affirm on the alternative basis of subparagraph (A), maintaining that a triable issue of fact exists as to Kaspersky's good faith. However, we have no need to consider subparagraph (A) immunity because we agree with the district court's disposition under subparagraph (B).

To the extent that Zango in reply raises a different issue — whether subparagraph (B), which has no good faith language, should be construed implicitly to have a good faith component like subparagraph (A) explicitly has — the argument is waived. *See Eberle*, 901 F.2d at 818. For present purposes, we

[9]These subparagraphs declare it to be the policy of the United States "(1) to promote the continued development of the Internet and other interactive computer services and other interactive media; [and] (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."

note that subparagraph (B) comes with only one constraint: the protection afforded extends only to providers who "enable or make available to . . . others" the technical means to restrict access to material that either the user *or* the provider deems objectionable.[10]

Conclusion

[8] The district court correctly held that Kaspersky is a provider of an "interactive computer service" as defined in the Communications Decency Act of 1996. We conclude that a 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. As its software qualifies, Kaspersky is entitled to good samaritan immunity.

AFFIRMED.

FISHER, J., Circuit Judge, concurring:

I concur with my colleagues that the plain language of the Communications Decency Act's "good samaritan" immunity provision, 47 U.S.C. § 230(c)(2)(B), given the way Zango has framed its appeal, compels us to affirm the district court's judgment that Kaspersky is immune from liability. Nonetheless, extending immunity beyond the facts of this case could pose serious problems if providers of blocking software were

[10]Zango's additional argument in reply that the proposed SPY Act (H.R. 964, 110th Cong. (2007)) supports its position is waived. We do not consider it, or Kaspersky's alternative argument that Zango fails on the merits to state a claim under Washington law.

to be given free license to *unilaterally* block the dissemination of material by content providers under the literal terms of § 230(c)(2)(A). The risk inheres in the disjunctive language of the statute — which permits blocking 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" — and the unbounded catchall phrase,"otherwise objectionable." *See* § 230(c)(2)(A), (B).

Kaspersky is an "access software provider that provides or enables computer access by multiple users to a computer server," § 230(f)(2), and its sale of blocking software is an "action taken to enable or make available to information content providers or others the technical means to restrict access" to Zango, which Kaspersky considers "otherwise objectionable," § 230(c)(2)(A), (B). Arguably, Zango's software is not "otherwise objectionable" under § 230(c)(2), but Zango waived that argument here.[1] Congress plainly intended to give computer users the tools to filter the Internet's deluge of material *users* would find objectionable, in part by immunizing the providers of blocking software from liability. *See* § 230(b)(3). But under the generous coverage of § 230(c)(2)(B)'s immunity language, a blocking software provider might abuse that immunity to block content for anticompetitive purposes or merely at its malicious whim, under the cover of considering

[1]Amici for both parties, listed above, Op. at 7980 n.4, argued for some limitation on Kaspersky's ability to declare Zango's product objectionable. Zango's amicus argued that the principle of *ejusdem generis* requires us to define "otherwise objectionable" by reference to the statute's other descriptions of objectionable material. By Zango's amicus' reading, Zango's software could be "otherwise objectionable" only if it were akin to "obscene, lewd, lascivious, filthy, excessively violent, [or] harassing" material. 42 U.S.C. § 230(c)(2)(A). Zango did not adopt this argument. Kaspersky's amici argued for an implicit good faith limitation, such that providers of access software like Kaspersky would be immune for blocking material they consider objectionable only when that blocking is in good faith. Zango made this argument only in reply and thus waived it.

such material "otherwise objectionable." Focusing for the moment on anticompetitive blocking, I am concerned that blocking software providers who flout users' choices by blocking competitors' content could hide behind § 230(c)(2)(B) when the competitor seeks to recover damages. I doubt Congress intended § 230(c)(2)(B) to be so forgiving. *Cf. Doe v. GTE Corp.*, 347 F.3d 655, 660 (7th Cir. 2003) ("Why should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?").

When presented at oral argument with the possibility § 230(c)(2)(B) could immunize covert blocking of content the user would want to access — if the user knew about it — Kaspersky emphasized that its software, Kaspersky Internet Security ("KIS"), when properly functioning, warns the user that KIS is about to block content. A pop-up window appears, and the user may "allow" the content over KIS's warning by clicking the appropriate button. But Kaspersky conceded that immunity under § 230(c)(2)(B) does not depend on the presence of such a warning or override option. Other blocking software might be less accommodating to the user's preferences, either not providing an override option or making it difficult to use. Consider, for example, a web browser configured by its provider to filter third-party search engine results so they would never yield websites critical of the browser company or favorable to its competitors. Such covert, anticompetitive blocking arguably fits into the statutory category of immune actions — those taken by an access software provider to provide the technical means to block content the *provider* deems objectionable.[2] Unless § 230(c)(2)(B) imposes some good faith limitation on what a blocking software provider can consider "otherwise objectionable," or some

[2]Not every software provider is an "access software provider" under the statute, but it seems the provider of a web browser would be; most web browsers come equipped with a filtering function, i.e., the technical means to "filter, screen, allow, or disallow content." § 230(f)(4)(A).

requirement that blocking be consistent with user choice, immunity might stretch to cover conduct Congress very likely did not intend to immunize.[3]

Computer users are of course always free to replace their blocking software with software more in line with their preferences, and this market-based solution finds support in the statute. *See* § 230(b)(2). But my concern is that blocking software providers — providers of web browsers being the most convenient and familiar example — could employ their software to block content for anticompetitive purposes *without the user's knowledge*. If users are unaware of undesired blocking, they would not know to switch to different software or even to complain to the blocked provider that they are having trouble accessing its material, thereby tipping off the content provider such as Zango alleges happened here when its users complained.

[3]The parties cite legislative history suggesting that one of § 230's chief purposes was to facilitate parents' and employers' efforts to control the influx of online content into the home and workplace by removing legal barriers to private filtering technologies, especially with respect to a provider's status as speaker or publisher under defamation law. *See, e.g.*, 141 Cong. Rec. H8470 (daily ed. Aug. 4, 1995) (statements of Rep. Cox and Rep. Wyden); *see generally Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (unpublished) (finding PRODIGY liable to plaintiff for libel because PRODIGY exercised editorial control over its online message boards). We recently reaffirmed that protecting Internet companies from liability arising out of their status as a speaker or publisher is at the heart of § 230 immunity. *See Barnes v. Yahoo!, Inc.*, 565 F.3d 560, 564-66 (9th Cir. 2009) (construing § 230(c)(1)).

As today's opinion makes clear, however, immunity under § 230(c)(2)(B), as opposed to (c)(1), is aimed at providers of blocking software and does not hinge on the defendant's speaking or publishing content. Thus, the legislative history the parties cite is not helpful in determining the exact boundaries of what Congress intended to immunize. Whatever those exact boundaries, I doubt Congress intended to leave victims of malicious or anticompetitive blocking without a cause of action, and no party has affirmatively argued that it did.

In Congress' judgment, immunity is necessary to facilitate users' access to blocking software that makes Internet use "safer" than it otherwise would be. *See* § 230(b)(4). It would be an abuse of this immunity to apply it to blocking activity of the kind I have hypothesized here. Nevertheless, until Congress clarifies the statute or a future litigant makes the case for a possible limitation, I agree that Kaspersky qualifies for immunity under this broadly worded statute.