No. 07-35800

IN THE
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ZANGO, INC.,
Plaintiff-Appellant,

v.

KASPERSKY LAB, INC.,
Defendant-Appellee.

On Appeal from the United States District Court
for the Western District of Washington

BRIEF AMICI CURIAE OF THE ANTI-SPYWARE COALITION, BUSINESS SOFTWARE ALLIANCE, CAUCE NORTH AMERICA, INC., CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC FRONTIER FOUNDATION, McAFEE, INC., PC TOOLS HOLDINGS PTY LTD, AND SUNBELT SOFTWARE, INC. IN SUPPORT OF APPELLEE AND AFFIRMANCE

John B. Morris, Jr.
Sophia Cope
CENTER FOR DEMOCRACY
& TECHNOLOGY
1634 I Street, NW, Suite 1100
Washington, D.C. 20006
(202) 637-9800

Counsel for Amici

May 5, 2008

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, counsel for *amici* certify the following:

Anti-Spyware Coalition ("ASC") is an unincorporated coalition of public interest organizations and companies. ASC is not a publicly-held corporation, does not have a parent corporation, and no publicly-held corporation owns 10 percent or more of its stock.

Business Software Alliance ("BSA") is a trade association. BSA is not a publicly-held corporation, does not have a parent corporation, and no publicly-held corporation owns 10 percent or more of its stock.

CAUCE North America, Inc. is a non-profit public interest organization. It is not a publicly-held corporation, does not have a parent corporation, and no publicly-held corporation owns 10 percent or more of its stock.

Center for Democracy & Technology ("CDT") is a non-profit public interest and Internet policy organization. CDT is not a publicly-held corporation, does not have a parent corporation, and no publicly-held corporation owns 10 percent or more of its stock.

Electronic Frontier Foundation ("EFF") is a non-profit public interest and Internet policy organization. EFF is not a publicly-held corporation, does not have a parent corporation, and no publicly-held corporation owns 10 percent or more of its stock.

McAfee, Inc. is a publicly traded company with no corporate parent. No publicly-held corporation owns 10 percent or more of its stock.

PC Tools Holdings Pty Ltd ("PC Tools") is not a publicly traded company, and has no parent corporations. Ellerston Capital Limited, a publicly traded company, owns in excess of 10 percent of the stock of PC Tools Holdings Pty Ltd. Ellerston Capital Limited is a wholly owned subsidiary of Consolidated Press Holdings Limited.

Sunbelt Software, Inc. is a non-public company that is a majority owned subsidiary of Sunbelt International Group, which it itself a non-public company. No publicly traded companies own 10 percent or more of either Sunbelt Software, Inc., or Sunbelt International Group.

TABLE OF CONTENTS

TABLE OF CASES AND AUTHORITIES

Cases:

Statutes, Public Laws and Legislative Materials:

Other Authorities and Material:

No. 07-35800

IN THE
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ZANGO, INC.,
Plaintiff-Appellant,

v.

KASPERSKY LAB, INC.,
Defendant-Appellee.

BRIEF AMICI CURIAE OF THE ANTI-SPYWARE COALITION, BUSINESS SOFTWARE ALLIANCE, CAUCE NORTH AMERICA, INC., CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC FRONTIER FOUNDATION, McAFEE, INC., PC TOOLS HOLDINGS PTY LTD, AND SUNBELT SOFTWARE, INC. IN SUPPORT OF APPELLEE AND AFFIRMANCE

INTEREST OF AMICI AND BACKGROUND

Pursuant to a motion under Fed. R. App. P. 29, this brief *amici curiae* is submitted on behalf of a broad spectrum of Internet and technology industry groups, public interest organizations, and individual companies that are all committed to the proposition that users should be empowered to control their own Internet experiences. With an enormous diversity of content on the Internet, *amici* believe that users should be able to choose and control what content is displayed on their screens. The individual *amici* are

identified and described in the "Identity of Amici" section following the Conclusion of this brief.

Many *amici* are particularly focused on providing users with software and technology tools with which to control "spyware," "adware," "viruses," and other categories of content that most (if not essentially all) users deem to be undesirable and unwanted. Many *amici* are industry leaders in the development of "anti-spyware" software. Other *amici* are more broadly concerned with empowering users with the ability to mold and adapt their Internet experiences to suit their personal – and family or corporate – preferences and values. Together, all *amici* believe that it is the user who should be able to decide what content displays and what software operates on his or her computer.

Working against the goal of user control is the widespread scourge of spyware and other unwanted content. Research has found that (as of 2005) almost half of all American adult Internet users reported that spyware or adware had been installed on their computers, more than two-thirds reported computer problems consistent with problems caused by spyware or viruses, and nine out of ten users had altered their online behavior because of fear of

such unwanted content.[1] In response to these fears and threats, more than 80 percent of American Internet users reported (as of 2007) that they installed "anti-spyware" software, and two-thirds actively use such software to block or remove unwanted content.[2]

Many *amici* have collaborated with the *amicus* Anti-Spyware Coalition ("ASC") to build a consensus among companies, academics, and consumer groups about definitions and best practices in efforts to resist spyware and other unwanted content. Collectively, the ASC works to help consumers better defend their computers against unwanted content and technologies, improve communication about what constitutes spyware and how anti-spyware companies combat it, and offer proposals for strengthening anti-spyware technology globally. All *amici* support the ability of users to acquire and use software tools to control their Internet experiences and limit spyware, adware, and other unwanted content.

---

[1] "Spyware: The threat of unwanted software programs is changing the way people user the internet," Pew Internet & American Life Project, July 6, 2005, available at http://www.pewinternet.org/PPF/r/160/report_display.asp.

[2] "Net threats: Why going online remains risky," Consumer Reports, Sept. 2007, available at http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07/overview/0709_net_ov.htm.

ARGUMENT

In enacting Section 230 of the Telecommunications Act of 1996, 47 U.S.C. § 230, Congress expressly identified a key policy objective (among others) of the provision: "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet . . . ." 47 U.S.C. § 230(b)(3). The question presented by this case is whether providers of technology tools and services that do just that – "maximize user control over what information is received" over the Internet, in this case "spyware" – are protected from liability under Section 230. For the reasons set out below, *amici* respectfully submit that the answer is "yes": Section 230 furthers the objectives of Congress by protecting providers of such tools and services against lawsuits that second guess their efforts to maximize user control.

I. IN ENACTING SECTION 230 CONGRESS SOUGHT TO FURTHER THREE DISTINCT AND INDEPENDENTLY IMPORTANT GOALS, INCLUDING MAXIMIZING "USER CONTROL" OVER THE INTERNET EXPERIENCE.

Although Section 230 is one of the most important sections of our nation's communications policy, not all parts of the section have received intensive focus. When Congress enacted Section 230, it articulated and pursued *three* distinct legislative goals. In its brief, Appellant Zango only emphasizes one of the three goals, and Zango ignores the goal most relevant

here – the goal "to encourage the development of technologies which maximize user control over what information is received." In deciding the issues presented in this case – and in understanding the prior discussions of Section 230 by this Court and others – it is vital that the Court understand *all three* of Section 230's goals. Because they have received the lion's share of judicial attention (and attention in Zango's brief), subparts I.A. and I.B. below will briefly describe the goals and relevant provisions of the two more prominent portions of Section 230. Subpart I.C. will then discuss in greater detail the critical goal and statutory language that is central to this appeal.

In addition to understanding the three distinct goals in Section 230, it is also important to recognize the broader legislative context in which Section 230 arose. As discussed below, Section 230 was initially introduced, in part, as an alternative to the proposed Communications Decency Act (the "CDA"), a bill aimed at restricting minors' access to online sexual content. But both as introduced and ultimately enacted, Section 230 had broader purposes, and it first arose in the context of a much larger legislative effort – communications policy reform that resulted in the Telecommunications Act of 1996, which had as one of its key purposes to "encourage the rapid deployment of new

telecommunications technologies."[3] Ultimately, Congress decided to enact *both* the CDA *and* Section 230 as part of the omnibus Telecommunications Act (and Section 230 ended up being placed within the previously separate CDA provisions),[4] and the three purposes of Section 230 reflect this broad heritage.

A. As Seen in the Most Familiar Applications of Section 230, Congress Sought to Promote a Vibrant and Unfettered Market for Internet Content and Services.

One central goal of Section 230 is to foster, promote, and protect the continued rapid development of the Internet, and content and services delivered over the Internet, unfettered by state and most federal regulation. It is this goal – which is pursued and implemented in the operative provisions found in Section 230(c)(1) – that has been at issue in the vast majority of litigated cases arising under Section 230. The goals underlying subsection 230(c)(1) provide the key to understanding the multitude of Section 230 decisions that have developed into a body of law.

---

[3] Preamble, Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

[4] *See id.* §§ 501 *et seq.* (CDA), 509 (Section 230).

For what is a relatively brief code section, Section 230 contains two detailed statements of goals – a "findings" section with five provisions, and a "policy" section also with five provisions. Section 230's first goal is seen in four of the five findings in 47 U.S.C. § 230(a):

> The Congress finds the following:
>
> (1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.
>
> …
>
> (3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
>
> (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.
>
> (5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

47 U.S.C. §§ 230(a)(1), (3), (4) & (5). These four findings emphasize the rapid development and dramatic potential of a diversity of Internet content and services. These findings are reflected in two of the five statements of policy found in Section 230(b):

> It is the policy of the United States—
>
> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
>
> (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 . . . .

Id. §§ 230(b)(1), (2). These two policies in turn are implemented in the first of the operative provisions of Section 230, found in 47 U.S.C. § 230(c)(1):

> (1) Treatment of publisher or speaker
>
> 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.

Taken together, these four findings, two policies, and one operative provision (coupled with the preemption of state laws found in Section 230(e)(2)), clarify and implement a core goal of Congress: to promote a diverse, competitive, and largely unregulated market for Internet content and services.

The operative provision – Section 230(c)(1) – addresses a critical potential barrier to the continued rapid development of the diversity of Internet content and services that Congress found so vital and beneficial. Section 230(c)(1) ensures that Internet service and content providers can allow users to participate in the collaborative process of content development, without the fear of a constant stream of lawsuits trying to hold the service

provider liable for content posted by others. Simply put, without the protections afforded by Section 230(c)(1), some of the most dynamic and popular video sharing, blogging, and other user-generated content sites on the Internet could not flourish – and may not have even been created.

It is this part of the statute – § 230(c)(1) – that is the focus of the vast majority of Section 230 cases to date, including *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998), *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003), *cert. denied* 541 U.S. 1085 (2004), and others. Although these cases have served the goals of Congress well, and are relevant to the general broad scope of Section 230 as a whole, the goals and specific terms of Section 230(c)(1) are *not* directly on point on the issues raised in *this* case. But because so many of the leading Section 230 cases address § 230(c)(1) – and because Zango and the *amicus* supporting Zango rely on these cases – it is important for the Court to recognize the goals and impact of this initial provision.

B. Congress Also Sought in Section 230 to Remove Disincentives for Service Providers to Take Voluntary Steps to "Self-Regulate" Content on the Internet.

In its brief, Zango focuses almost exclusively on the second of the three goals of Section 230 – the removal of disincentives for service providers to take voluntary steps to "self regulate" content on the Internet. As is clearly

stated in the minimal legislative history of Section 230[5], *one* of the goals of the provision was to overrule the 1995 court decision in *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. 1995), which imposed liability on Prodigy because it took some steps to "filter" out objectionable online content. But, like Section 230(c)(1) discussed above, this goal of Section 230 is *also* not the one that is central to this appeal. Nevertheless, it is important for the Court to recognize this independent goal.

This second goal is directly anticipated in the one of the five statements of policy found in Section 230(b):

> It is the policy of the United States—
>
> (4) 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 …

47 U.S.C. § 230(b)(4). This policy in turn is implemented in the second operative provision of Section 230, found in subsection (c)(2)(A):

---

[5] *See* H.R. Conf. Rep. No. 104-458, at 207-08 (1996).

(2) Civil liability

> 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). This provision effectively addresses the second goal: to remove disincentives to voluntary screening by service providers created by the *Stratton-Oakmont* decision.

C. Critical to this Case, Congress Also Enacted Section 230 to "Encourage the Development of Technologies Which Maximize User Control" Over Users' Internet Experience.

In addition to wanting to broadly promote the continued rapid and innovative development of the Internet (the first goal in Section 230) and to remove disincentives to self-screening of content (the second goal), Congress had a *third* goal in enacting Section 230: to promote the development of "user control" technologies. As H.R. 1978 – the legislative source of Section 230 – termed it, the provision was to be called the "Internet Freedom and

Family Empowerment Act."[6] It is this third goal of empowering users that is central to this appeal (and is overlooked by Zango).

In anticipation of the explosion of diverse online content that Congress hoped to foster through Section 230(c)(1) (pursuing the first goal), Congress knew that the best way to shield users from undesired content was to promote "user empowerment" technology tools that allow users to control their Internet experiences. User empowerment and control tools are critically valuable for Internet users because (a) users can tailor the technology tools to meet their particular needs (instead of "one-size-fits-all" government mandates or regulation), and (b) users can use such tools to control content coming from outside of the United States (and thus generally outside of the reach of direct Congressional regulation of Internet content). A broad range of independent studies and court decisions have confirmed that "user empowerment" tools are a vital component (along with education and enforcement of existing criminal laws) to shield users from undesired

---

[6] Internet Freedom and Family Empowerment Act, H.R. 1978, 104th Cong., 1st Sess. (1995) (emphasis added), available at http://thomas.loc.gov/cgi-bin/query/z?c104:h.r.1978:.

content.[7] Congress sought in Section 230 to encourage further development of user control technologies.

This third goal is seen in one of the five findings in Section 230(a):

> The Congress finds the following:
>
> > (2) These services offer users a great degree of control over the information they receive, as well as the potential for even greater control in the future as technology develops.

47 U.S.C. § 230(a)(2). This finding – applauding the concept of "user control" – is central to one of the five statements of policy found in Section 230(b):

> It is the policy of the United States—
>
> > (3) 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 . . . .

---

[7] *See, e.g., Amer. Civil Liberties Union v. Gonzales*, 478 F. Supp. 2d 775, 789-97 (E.D. Pa. 2007), *appeal pending*, No. 07-2539 (3d Cir.); "Youth, Pornography, and the Internet," Nat'l Research Council of the Nat'l Academy of Sciences, (2002), available at http://books.nap.edu/html/youth_internet/; "Final Report," COPA Commission (2000), available at http://www.copacommission.org/report/.

Id. § 230(b)(3) (emphasis added). This policy is in turn implemented in the second part of the second operative provision of Section 230, found in 47 U.S.C. § 230(c)(2)(B):

> (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 material described in [§ 230(c)(2)(A)].[8]

This final provision of Section 230(c) was aimed at protecting the providers, developers, and distributors of user control tools. That Section 230(c) is intended to protect the creators of user control tools is confirmed in the "Definitions" section of Section 230. Section 230(f)(4) expressly extends the protections of Section 230 to:

---

[8] Although the enacted text of Section 230(c)(2)(B) refers to "material described in paragraph (1)," the codifiers note that this was a drafting mistake and the reference should be to subparagraph (A). This conclusion confirmed by reference to the original legislative source of Section 230. *See* H.R. 1978, 104th Cong., 1st Sess. (1995) (emphasis added), available at http://thomas.loc.gov/cgi-bin/query/z?c104:h.r.1978:.

> 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; or
> (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

47 U.S.C. § 230(f)(4), so long as such provider allows "multiple users [access] to a computer server," *id.* § 230(f)(2). (This later requirement is discussed in more detail in Part II.B. below.)

Promoting the development of user control tools is a distinct goal from promoting the Internet more generally (as is done in Section 230(c)(1)) or overturning the *Stratton-Oakmont* disincentive for self-regulation (as is done in § 230(c)(2)(A)). It is this goal – as pursued in Section 230(c)(2)(B) – that is at issue in this case.

II. PROVIDERS OF "ANTI-SPYWARE" SOFTWARE AND SERVICES ENABLE THE TYPE OF "USER CONTROL" THAT CONGRESS SOUGHT TO PROMOTE AND PROTECT IN SECTION 230, AND SUCH PROVIDERS ARE WITHIN THE SCOPE OF SECTION 230'S PROTECTIONS.

Spyware, adware, spam, and sexual images are all examples of content that many (and in some cases almost all) Internet users want to control. But, although the most common type of "user empowerment" software available in the mid-1990s when Section 230 passed was software to control access to sexual images, Congress did not intend for Section 230's promotion of "user

control" technologies to be limited only to promoting those technologies that block access to sexual content. And as objectionable content on the Internet has evolved, so have user control tools. Today many such tools include "suites" of programs that offer users control over a broad range of types of content – including "spyware" and "adware."[9]

The district court in this case grappled with the question of whether a provider of anti-spyware software and services would be covered by the protections in Section 230(c)(2)(B). Although the undersigned *amici* diverge from the lower court on one point (discussed in Section II.C.), *amici* respectfully urge this Court to find that anti-spyware vendors (like Appellee Kaspersky Lab) fall under the protections of Section 230, for the reasons detailed below.

---

[9] Different anti-spyware software vendors – including various *amici* here – categorize the content and software currently distributed by appellant Zango in differing manners – some place Zango in the "spyware" category, while others place Zango in the "adware" category. Both of these categories, however, are among the types of unwanted content (along with other types of objectionable content such as viruses and spam) that anti-spyware tools are designed to empower users to block, remove, or disable.

A. "Spyware" is Within the Type of "Objectionable" Content that Congress Wanted Users to Be Able to Control Pursuant to Section 230(c)(2)(A).

When Congress enacted Section 230, it was in the context of the debate about the then-proposed Communications Decency Act ("CDA"), and Congress's main focus was on methods to shield children from sexual content. But Congress purposefully refrained from confining Section 230's reach to sexual content, and instead stated a broader goal "to encourage the development of technologies which maximize user control over what information is received" *without limiting* Section 230 to only promoting control over objectionable sexual content.

Amicus National Business Coalition on E-Commerce and Privacy ("NBCEP"), in support of Zango, emphasizes the doctrine of *ejusdem generis* to argue that Section 230 should be narrowly construed in its reach (and essentially, should only apply to sexual content). This argument fails for at least two reasons. First, the plain language of Section 230 is broader than the words used elsewhere in the Telecommunications Act (including the CDA), indicating that Congress intended Section 230 to reach beyond the sexual focus of the CDA. The CDA addressed Congressional concerns about "obscene, lewd, lascivious, filthy, or indecent" content, while Section 230(c)(2)(B) promotes tools that allow user control over "obscene, lewd,

lascivious, filthy, *excessively violent, harassing, or otherwise objectionable*" content (emphasis added).[10] By including violent and harassing content, Congress made clear that it was reaching beyond sexual content and more broadly promoting user empowerment tools.

Second, *ejusdem generis* does not in any event apply because spyware comfortably fits one of the "specific words" used in the statutory text: "harassing." One aspect of some spyware is that it causes "pop-up" advertisements and other nagging and bothersome windows to open on computers that contain spyware and "adware." Such actions are indeed – at least to many users of anti-spyware services – "harassing." Given the harassing nature of some spyware, it comfortably fits into the category of content that can appropriately be controlled by "user control" tools promoted by Section 230.[11] As other courts have found, the statutory list of content

---

[10] *Compare* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996), § 502 (CDA, codified at 47 U.S.C. § 223) *with* § 509 (Section 230(c)(2)(A)).

[11] Although the undersigned counsel is unable to locate a current membership list of NBCEP in court filings in this case or on any website, a 2004 agency filing, *see* http://www.ftc.gov/os/comments/canspam/OL-105261.pdf, reveals that NBCEP is comprised mainly of data collection companies that support advertising & tracking systems on the Internet, and corporate advertisers that use such advertising & tracking systems. Some of the member companies of

(footnote continued)

covered by Section 230 is not confined to sexual or other narrow category of content. *See Langdon v. Google, Inc*., 474 F.Supp.2d 622, 631 (D. Del. 2007) (broadly construing "otherwise objectionable" in Section 230(c)(2)); *e360Insight, LLC v. Comcast Corp.*, 2008 WL 1722142 (N.D. Ill. Apr. 10, 2008) (same).

B. Providers of "Anti-Spyware" Software and Services are "Providers or Users" of "Interactive Computer Services" as Protected under Section 230(c)(2).

In Section 230, Congress did not narrowly cabin the types of technical user control tools that it sought to promote – instead, Congress aimed at encouraging the development of a broad range of such tools, using various technical architectures. The statutory language quoted above – from

---

NBCEP may provide or use technology to surreptitiously "track" users' web surfing and deliver advertisements, and many of the anti-spyware services and tools alert and warn users about these tracking programs, and allow users to disable such tracking and ad-delivery programs. Although advertisers likely believe that their ads are interesting and valuable to end users (and that tracking users' websurfing on the Internet enhances their ads), many users believe that tracking software, "adware," pop-up advertisements, and other forms of spyware that infringe their expectations of privacy and control over their own computer are "harassing" and "objectionable." Tools that enable those users to control such harassing content are covered within the reach of Section 230(c)(2).

Section 230(c)(2) & 230(f)(4) – anticipates more than one technical approach to empowering users.

Moreover, the technical architecture at issue in this case is the *exact* same as was in use when Section 230 was passed. In 1995 and early 1996, when Congress was working to promote the development of user empowerment tools, the leading such products in the marketplace (such as CyberPatrol and SurfWatch, both mainly aimed at sexual content) used an architecture in which client-side software (installed on each users' individual computer) would "phone home" to a centralized server to obtain updated lists of content to filter or block. In the 1996 legal challenge to the Communications Decency Act, the three-judge district court described in its Findings of Fact how CyberPatrol's "CyberNOT" filtering list was automatically updated by its creator, Microsystems:

> 58. Microsystems employs people to search the Internet for sites containing material in these categories [of content to be filtered]. Since new sites are constantly coming online, Microsystems updates the CyberNOT list on a weekly basis. Once installed on the home PC, the copy of Cyber Patrol receives automatic updates to the CyberNOT list over the Internet every seven days.

ACLU v. Reno, 929 F. Supp. 824, 840-41 (E.D. Pa 1996), *aff'd*, 521 U.S. 844 (1997). This technical architecture – with "client-side" software installed on users' computers automatically "phoning home" to a server to obtain updated

blocking lists – is the *exact* architecture that is in use today both in the area of sexual-content filtering *and* in the area of spyware control. As the *Reno* court noted, the reason for this architecture is clear – just as new websites with sexual content are created every day, so are new "spyware" threats created every day. To respond in both cases, the client-side software connects back to a home server to obtain new lists of content to watch for and control. This architecture is at the core of the technology that Congress was specifically trying to promote in Section 230.

Nevertheless, Zango and *amicus* NBCEP assert that this architecture does not meet the terms of Section 230, primarily based on the fact that both Congressional and judicial discussion of Section 230 have focused on traditional content providers (in the context of the first two goals of Section 230), and no court to date has addressed this architecture in the context of Section 230. Yet these facts are hardly surprising given that this case involves the *third* goal, and the *third* operative provision of Section 230, both aimed at promoting and protecting the development of user empowerment tools themselves. To *amici's* knowledge, this case is the first federal appellate case to address the scope of Section 230(c)(2)(B) in the context of a creator of "user empowerment" tools.

However, a handful of courts have examined Section 230(c)(2) in different contexts. In *Pallorium v. Jared*, 2007 WL 80955, (Cal. Ct. App. 2007), the California Court of Appeal examined Section 230(c)(2)(B) in the context of a filter for email, and determined in an unpublished opinion that the provider of a filtering list for unwanted e-mail was an "interactive computer service." *Id.* at *7. While the unpublished opinion is not precedent in California courts, it remains persuasive.[12]

There is no inconsistency between the district court's holding and the goals, intent, and most critically, the text of Section 230. There can be no dispute that an anti-spyware service provider is a "provider of software (including client or server software), or enabling tools that . . . filter, screen, allow, or disallow content . . . ," 47 U.S.C § 230(f)(4), and therefore is an "access software provider." Thus, the only question is whether the architecture described above (in which many end users regularly retrieve a filtering list from a central server) meets the requirement that the access software provider "provide[] or enable[] computer access by multiple users to

---

[12] Similarly, last month a federal district court in Illinois applied Section 230(c)(2) to shield a Internet service provider from liability for blocking spam e-mail. See *e360Insight, LLC v. Comcast Corp.*, 2008 WL 1722142 (N.D. Ill. Apr. 10, 2008).

a computer server" pursuant to Section 230(f)(2). The district court correctly applied the straightforward meanings of those words to find that the technical architecture of a typical anti-spyware service provider comfortably fits within the statutory language.

C. The Protections Afforded by Section 230(c)(2) Are Inherently Limited to Legitimate Providers of Tools That In Fact Empower Users.

Amici agree with the result and most of the analysis of the lower court in this case, but *amici* do diverge somewhat from the district court's implicit suggestion that the protections of Section 230(c)(2)(B) might extend to a maker of "user control" that is acting in bad faith. As the district court correctly noted, Section 230(c)(2)(B) by its terms does not include an express "good faith" requirement (in contrast to Section 230(c)(2)(A)). Nevertheless, *amici* believe that inherent in the text of and purpose behind Section 230(c)(2)(B), is an intention that the protection provided by that subsection can only extend to software and service providers who are truly seeking to empower users to exercise control over objectionable content received over the Internet (as opposed to pursuing, for example, fraudulent or anti-competitive objectives).

A look at both parts of Section 230(c)(2) finds that a service provider must be providing a tool that, in fact, empowers users before it can benefit

from either part of Section 230(c)(2). For Section 230(c)(2)(A), a good faith requirement is expressly stated. This express inclusion of good faith makes sense in light of the authority given by subsection (A) to service providers: a service provider (such as, for example, AOL providing access to the Internet) is permitted to block access to content *without the consent of the end user of the service*. Under its terms, the provider can block access to "material that the *provider or* user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" (emphasis added). Given that authority, Congress understandably wanted to ensure that providers would only be protected by Section 230 if they block access to content *in good faith*, and not for anti-competitive or fraudulent reasons.

In contrast, Section 230(c)(2)(B) only protects entities that provide the tools and services to enable *others* to block access to content – in other words, to empower users to control access to Internet content. Inherent in this provision is the requirement – effectively an implicit "good faith" requirement – that the tool or service must truly be empowering users to do something *the users want to do* (such as filtering out sexual content, or blocking spyware content). Section 230(c)(2)(B) protects providers of legitimate user control/empowerment tools and services that genuinely give *users* the "means to restrict access to [objectionable] material." The leading

vendors of anti-spyware software and services (and the Appellee Kaspersky Lab is one such vendor) provide users with the means to block objectionable content, and are thus protected under Section 230(c)(2)(B).

Under this inherent requirement in Section 230(c)(2)(B), anti-competitive and fraudulent actions would not be protected. Thus, hypothetically, if a broadband access provider that also provides cable TV video services (as increasingly most broadband providers do) were to create a "tool" that blocked users access to online video sites (such as YouTube.com) without the users' awareness or consent, then such provider would not be protected under this subsection. Similarly, if a spyware maker distributes software that causes harassing advertisements to "pop-up" on users' screens, and then the same software offers to block the harassing pop-ups (for payment of a fee), the software would not be protected under this subsection because the fraudulent installation of the harassing advertisements in the first place would not be covered by the statutory language. What is critical is that tools and services covered by Section 230(c)(2)(B) must truly be empowering *users* to control content.

User choice, however, is a more complicated issue than the arguments advanced by Zango and *amicus* NBCEP would suggest. Both briefs assert – without any foundation, as far as the undersigned *amici* are aware – that

Appellee Kaspersky Lab is taking action against the wishes of its users. Zango claims that consumers have "consented" to the installation of Zango's software. Whether that is true or not,[13] the assertion that someone might "consent" to the download of Zango software does *not* indicate that Kaspersky Lab is taking any action contrary to the wishes of its users, or that Kaspersky Lab is somehow not acting in good faith.

Two scenarios illustrate the interplay of "consent" in the anti-spyware context. First, assume that a user did consent to the installation of Zango software, but later concluded that the software and resulting advertisements were harassing and objectionable. Kaspersky Lab (and most anti-spyware services and tools) offers the ability to disable Zango software, and for a user to choose to install Kaspersky software to block Zango's advertisements is

---

[13] In the past, Zango (formerly known as 180solutions) engaged in practices that led to an investigation by the Federal Trade Commission of whether Zango in fact obtained the informed consent of users. That investigation resulted in a settlement and payment by Zango of a significant fine. *See* Decision & Order, *In the Matter of Zango, Inc. f/k/a 180Solutions, Inc.*, No. C-4186 (Fed. Trade Comm. Mar. 7, 2007), available at http://www.ftc.gov/os/caselist/0523130/index.shtm. *Amici* do not in this brief take any position as to whether Zango currently obtains the fully informed consent of its users.

fully consistent with the user's true choice (notwithstanding the assumed initial consent to install the Zango software).

Second, if the Kaspersky Lab software is installed on a computer *before* someone attempts to download and install the Zango software (and Kaspersky software blocks the Zango installation), that is quite possibly *also* fully consistent with the wishes of the user. By installing anti-spyware software, the user is asking to be protected from spyware *even if the user does not immediately recognize certain downloaded software as spyware*. Moreover, it may well be that the owner of the computer (such as a parent or an employer) decided to install anti-spyware software such as Kaspersky Lab's, and then some *other* users (such as a child or employee) attempts to install Zango software (and that installation is blocked). In that scenario, the anti-spyware software is in fact doing *precisely* the job that it was asked to do. (This is much like the real-world scenario of a company hiring a security guard to walk around the building to ensure that all doors are locked, *even* if an employee tries to prop open a door.)

Looking back at the history of Section 230, it becomes clear that a mere assertion that *someone* "consented" to the download of software such as Zango's does not take the situation outside of Section 230. A core goal of Section 230 is to empower *parents* to shield their children from certain

content – *even* where a child affirmatively "consents" to the receipt of that content. What is essential – in both the anti-spyware as well as the sexual-content-filtering contexts – is that the user empowerment tool must truly give users control (even if, in some cases, the "user" is the parent or employer who overrides the wishes of the child or employee).

Thus, *amici* strongly agree with the district court's ultimate conclusion – that a legitimate anti-spyware service provider (such as Kaspersky Lab) is protected by Section 230(c)(2)(B).

CONCLUSION

As detailed in Section I above, Congress had three purposes in enacting 47 U.S.C. § 230, the third of which was "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet . . . ." 47 U.S.C. § 230(b)(3). Congress embraced "user control" as a strong value, and Congress looked forward to "the potential for even greater control in the future as technology develops." 47 U.S.C. § 230(a)(2). In crafting Section 230(c)(2), Congress pursued that potential by protecting good faith providers of user control technologies that empower Internet users (including parents) to control what content they (and, in the case of parents, their children) receive over the Internet.

The most common technical architecture for user empowerment tools in the mid-1990s – having "client side" software regularly obtain from a central server updates of content to be filtered – is still in use today, and still easily fits within the definitions contained in Section 230. Providers of these tools – including tools aimed at controlling harassing content such as spyware – are covered by, and thus protected by, Section 230(c)(2)(B). A decision to the contrary would fail to give full meaning to the multi-faceted text of Section 230.

Congress sought to promote and protect "user empowerment" as the best way to protect users online. This Court should give effect to that Congressional goal as reflected in the text of Section 230, and should affirm the district court's decision.

IDENTITY OF THE AMICI

Anti-Spyware Coalition ("ASC") (www.antispywarecoalition.org) is an unincorporated coalition made up of leading anti-spyware providers as well as academics and public interest groups committed to combating the rise of unwanted spyware clogging computers and endangering Internet communications. It draws on the combined expertise of its members to help consumers better defend their computers against unwanted content and technologies, improve communication about what constitutes spyware and

how anti-spyware companies combat it, and offer proposals for strengthening anti-spyware technology globally.

Business Software Alliance ("BSA") (www.bsa.org) is a trade association dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. BSA promotes policies that foster technology innovation, growth, and a competitive marketplace for commercial software and related technologies. BSA members collectively provide information security products and services to consumers, businesses and governments, including solutions to empower Internet users to control their experience, and to allow them to protect themselves against unwanted or malicious software. As such, BSA members have a strong stake in this case. BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, CA, Cadence Design Systems, Cisco Systems, CNC Software/Mastercam, Corel, Dell, EMC, HP, IBM, Intel, McAfee, Microsoft, Monotype Imaging, PTC, Quark, Quest Software, SAP, Siemens PLM Software, SolidWorks, Sybase, Symantec, Synopsys, and The MathWorks.

CAUCE North America, Inc. (www.cauce.org) the Coalition Against Unsolicited Commercial Email, is a non-profit all-volunteer consumer

advocacy organization. It actively advocates on behalf of consumers to governments, legislators, law enforcement agencies and industry associations about matters related to the blended threat of spam, viruses and spyware, and engages in user and industry outreach and education about this threat.

The Center for Democracy & Technology ("CDT") (www.cdt.org) is a non-profit public interest and Internet policy organization. CDT represents the public's interest in an open, decentralized Internet reflecting constitutional and democratic values of free expression, privacy, and individual liberty. For its entire existence, CDT has actively promoted the use of "user empowerment" technology as the effective way to protect users from undesired content online. As part of that commitment to user empowerment, CDT manages (and helped to organize) the Anti-Spyware Coalition, which works to promote best practices within the anti-spyware industry. CDT has also worked to protect a broad interpretation of Section 230, and has participated as *amicus* in a range of cases involving that statute.

The Electronic Frontier Foundation ("EFF") (www.eff.org) is a non-profit, member-supported civil liberties organization that works to protect rights in the digital world. EFF encourages and challenges industry, government and the courts to support free expression, privacy, and openness in the information society. It is particularly concerned that laws and

regulations not be used to stifle user control of their computers and Internet experience. EFF supports a broad interpretation of Section 230 of the Communications Decency Act because this statute has played a vital role in advancing and enabling user control and free speech online. EFF has participated in a significant number of cases addressing the interpretation of this statute.

McAfee, Inc. ("McAfee") (www.mcafee.com) is a leading dedicated security technology company that develops and markets software tools and hardware for securing computer systems and networks from known and unknown threats around the world. Computer security is one of the most critical concerns facing businesses and consumers, fueled by the extraordinary proliferation of threats like viruses and spyware, the continuous evolution of threats against privacy, and the expansion of attack vectors in to mobile platforms like laptop computers and cell phones. Corporations rely on McAfee's tools to manage their computer security risks and compliance with expanding security related regulatory requirements. Consumers rely on McAfee's tools and judgment to help them identify and combat threats that would otherwise discourage them from using their computers or conducting transactions online. McAfee's products empower home users, businesses, government agencies, and other entities and organizations with the ability to

block attacks, prevent disruptions, screen content, and continuously track and improve their computer security.

PC Tools Holdings Pty Ltd ("PC Tools") (www.pctools.com) is a global software publisher of security and utility products and is an industry leader in anti-spyware software. Through its Malware Research Center, PC Tools monitors trends and emerging spyware issues affecting computer users. PC Tools is also a member of the Anti-Spyware Coalition. Shortly before suing Kaspersky, Zango sued and asserted the same claims against PC Tools Pty Ltd (a subsidiary of PC Tools Holdings Pty Ltd). The district court denied Zango's TRO motion against PC Tools Pty Ltd, and Zango voluntarily dismissed its lawsuit against PC Tools Pty Ltd.

Sunbelt Software, Inc. ("Sunbelt") (www.sunbelt-software.com) provides security solutions to enterprises, small businesses, schools, and government entities as well as home consumers. Sunbelt's primary anti-malware program, CounterSpy, protects users and administrators against all manner of potentially unwanted programs, including adware, spyware, malware, and greyware. Sunbelt a member of the Anti-Spyware Coalition. Sunbelt believes that in order to help users and administrators maintain control of their computer systems, anti-malware software vendors must be

responsive to the needs of their customers, offering protection against the wide range of software that undermines user privacy and security.

Respectfully submitted,

_____

John B. Morris, Jr.
Sophia Cope
CENTER FOR DEMOCRACY
& TECHNOLOGY
1634 I Street, NW, Suite 1100
Washington, D.C. 20006
(202) 637-9800

Counsel for Amici

Dated: May 5, 2008

CERTIFICATION OF COMPLIANCE PURSUANT TO FED. R. APP. P. 32(a)(7)(C) AND CIRCUIT RULE 32-1 FOR CASE NO. 07-35800

I certify that:

1. Pursuant to Fed. R. App. P. 32(a)(7)(C) and Ninth Circuit Rule 32-1, the attached brief *amici curiae* is:

Proportionally spaced, has a typeface of 14 points or more and contains 6,951 words, as determined by Microsoft Word 2004 for Mac, and excluding materials permitted to be excluded under Fed. R. App. P. 32(a)(7)(B)(iii).

_____
John B. Morris, Jr.

Dated: May 5, 2008

CERTIFICATE OF SERVICE

I hereby certify that on May 5, 2008, 15 copies of the foregoing *amicus* brief were filed with the Clerk of the Court, United States Court of Appeals for the Ninth Circuit, 95 Seventh Street, San Francisco, CA 94103, by overnight delivery service for next-day delivery, and two copies were shipped by commercial carrier for next-day delivery, or placed in U.S. Mail, postage prepaid, upon the following:

Jeffrey Tilden
Michael Rosenberger
Gordon Tilden Thomas
& Cordell, LLP
1001 Fourth Avenue, Suite 4000
Seattle, WA 98154
Counsel for Zango (by FedEx)

Erik Belt
Peter Karol
Bromberg & Sunstein LLP
125 Summer Street
Boston, MA 02110
Counsel for Kaspersky Lab (by FedEx)

Dimitri Nionakis
David Lieber
DLA Piper, LLP
500 8th Street, NW
Washington, DC 20004
Counsel for NBCEP (by U.S. Mail)

Bruce Johnson
Davis Wright Tremaine
1201 Third Avenue, Suite 2200
Seattle, WA 98101
Counsel for Kaspersky Lab (by FedEx)

_____
John B. Morris, Jr.