

No. 21-1333

In The
Supreme Court of the United States

—◆—
REYNALDO GONZALEZ, et al.,

Petitioners,

v.

GOOGLE LLC,

Respondent.

—◆—
**On Writ Of Certiorari To The
United States Court Of Appeals
For The Ninth Circuit**

—◆—
**BRIEF FOR INTERNET SOCIETY AS
AMICUS CURIAE SUPPORTING AFFIRMANCE**

—◆—
RAECHEL KEAY KUMMER
Counsel of Record
JAMES D. NELSON
MEREDITH L. COMPTON
MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Avenue, N.W.
Washington, DC 20004
(202) 739-3000
raechel.kummer@morganlewis.com

TABLE OF CONTENTS

	Page
TABLE OF CONTENTS	i
TABLE OF AUTHORITIES	iii
INTEREST OF AMICUS CURIAE	1
SUMMARY OF ARGUMENT	2
ARGUMENT	3
I. Through Section 230, Congress Expressly Sought to Protect and Enable a Medium for Unique Modes of Interactivity	4
A. Interactivity Has Been Key to Online Communications Since Before the Internet Became a Publicly Available Resource	5
B. Congress Protected the Interactivity of the Internet with Section 230	7
II. Far from Enshrining a “Traditional” Concept of Communications Regulation, Section 230 Created a Framework to Support the Internet’s Innovation	9
A. Section 230 Fosters Editorial Innovation.....	9
B. Section 230 Does Not Include a “Traditional Editorial Function” Standard	12
III. Section 230 Immunity Is Crucial to the Flourishing of Many Different Parts of the Internet Ecosystem.....	14
A. Section 230 Protection Is Essential	14

TABLE OF CONTENTS—Continued

	Page
1. The Internet’s infrastructure	14
2. The importance of intermediary immunity	19
B. Section 230 Protection Is Crucial to a Wide Range of Providers and Companies at Many Levels of the Stack	20
C. Section 230 Protection Is Vital for Individuals, Small Companies, and Non-profits	23
CONCLUSION.....	25

TABLE OF AUTHORITIES

	Page
CASES	
<i>Am. Civ. Liberties Union v. Reno</i> , 929 F. Supp. 824 (E.D. Pa. 1996).....	8
<i>Barnes v. Yahoo!, Inc.</i> , 570 F.3d 1096 (9th Cir. 2009).....	13
<i>Cubby, Inc. v. CompuServe Inc.</i> , 776 F. Supp. 135 (S.D.N.Y. 1991)	6
<i>Gonzalez v. Google LLC</i> , 2 F.4th 871 (9th Cir. 2021).....	13
<i>Nat’l Fed’n of Indep. Bus. v. Sebelius</i> , 567 U.S. 519 (2012).....	10
<i>Reno v. Am. Civ. Liberties Union</i> , 521 U.S. 844 (1997).....	7, 8
<i>Stratton Oakmont, Inc. v. Prodigy Servs. Co.</i> , 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995)	6
<i>Zango, Inc. v. Kaspersky Lab, Inc.</i> , 568 F.3d 1169 (9th Cir. 2009).....	22
<i>Zeran v. Am. Online, Inc.</i> , 129 F.3d 327 (4th Cir. 1997).....	13, 14
CONSTITUTIONAL PROVISIONS	
U.S. Const. amend. I	7

TABLE OF AUTHORITIES—Continued

	Page
STATUTES AND RULES	
47 U.S.C. 230	2-14, 17-25
Communications Decency Act.....	7
S. Ct. Rule 37.6	1
OTHER AUTHORITIES	
<i>A Brief History of NSF and the Internet</i> , National Science Foundation (Aug. 13, 2003), https:// www.nsf.gov/news/news_summ.jsp?cntn_id=1 03050	6
<i>Analytics Insight, Wikipedia employs AI to learn more about the issue its facing and consider possible solutions</i> , Swiss Cognitive (June 10, 2021), https://swisscognitive.ch/2021/06/10/ wikipedia-and-ai	12
Ashley Johnson & Daniel Castro, <i>Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved</i> , ITIF (Feb. 22, 2021), https://itif.org/publications/2021/02/22/ overview-section-230-what-it-why-it-was- created-and-what-it-has-achieved	7

TABLE OF AUTHORITIES—Continued

	Page
Chris Riley & David Morar, <i>Legislative efforts and policy frameworks within the Section 230 debate</i> , Brookings (Sept. 21, 2021), https://www.brookings.edu/techstream/legislative-efforts-and-policy-frameworks-within-the-section-230-debate/	10
David Belson, <i>Is the Internet Resilient enough to Withstand Coronavirus?</i> , Internet Society (Feb. 28, 2020), https://www.internetsociety.org/blog/2020/02/is-the-internet-resilient-enough-to-withstand-coronavirus	20
EarthData, <i>Data Tools</i> (Oct. 29, 2020), https://www.earthdata.nasa.gov/learn/use-data/tools	12
GitHub, https://github.com/	24
GitLab, https://about.gitlab.com/	24
<i>Intermediary Liability: The Hidden Gem</i> , Internet Society (Mar. 11, 2020), https://www.internetsociety.org/blog/2020/03/intermediary-liability-the-hidden-gem	19
Internet Society, <i>Internet Way of Networking Use Case: Intermediary Liability</i> (Sept. 9, 2020), https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-intermediary-liability/	15, 17, 18, 22, 23

TABLE OF AUTHORITIES—Continued

	Page
Joe Biden, <i>Republicans and Democrats, United Against Big Tech Abuses</i> , WSJ Opinion (Jan. 11, 2023), https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrust-children-algorithm-11673439411	10
Lawrence B. Solum & Minn Chung, <i>The Layers Principle: Internet Architecture and the Law</i> , 79 NOTRE DAME LAW REV. 815 (2004)	15, 16
Press Release, House Committee on Energy & Commerce, E&C Leaders Announce Legislation to reform Section 230 (Oct. 14, 2021), https://energycommerce.house.gov/newsroom/press-releases/ec-leaders-announce-legislation-to-reform-section-230	10
Saurav Mohapatra, <i>MaRS: How Facebook keeps maps current and accurate</i> , Engineering at Meta (Sept. 30, 2019), https://engineering.fb.com/2019/09/30/ml-applications/mars	12
<i>The TCP/IP stack</i> , Isaac Computer Science, https://isaacomputerscience.org/concepts/net_internet_tcp_ip_stack?examBoard=all&stage=all	16
Vint Cerf, <i>A Brief History of the Internet and Related Networks</i> , Internet Society, https://www.internetsociety.org/internet/history-internet/brief-history-internet-related-networks/	5
World Intermediary Liability Map, https://wilmap.stanford.edu	19

INTEREST OF AMICUS CURIAE¹

Founded in 1992, the Internet Society is a U.S. non-profit organization headquartered in Reston, Virginia, and Geneva, Switzerland, for the worldwide coordination of, and collaboration on, Internet issues, standards, and applications. The Internet Society's staff is comprised of technical experts in internetworking, cybersecurity, and network operations, among other fields, as well as policy experts in a broad range of Internet-related areas.

As a global non-governmental organization, the Internet Society believes that the Internet should be for everyone. It supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society, with an overarching goal that the Internet be open, globally connected, secure, and trustworthy. The Internet Society supports communities that seek to connect to each other through the Internet. It advances the development and application of Internet infrastructure, technologies, and open standards. The Internet Society also advocates for policies that protect the Internet and allow it to flourish for all.



¹ In accordance with this Court's Rule 37.6, amicus states that no counsel for a party authored this brief in whole or in part, and that no person other than amicus, its members, or its counsel made a monetary contribution intended to fund its preparation or submission.

SUMMARY OF ARGUMENT

The Internet is a novel medium—from its unique people-driven interactivity to the speed of its growth to its groundbreaking innovations over time. Congress recognized the Internet’s potential to drastically improve the ability of citizens to communicate and interact with each other, and Congress sought to promote and protect the Internet’s distinguishing features through Section 230. This Court should not upend those protections.

First, from the beginning, the Internet was a fundamentally interactive place—where individuals actively participate in public discourse, rather than merely consume it. Participants may interact with other individuals or with the wider public in ways never before imagined. Congress preserved and encouraged this interactivity through the intermediary protections of Section 230.

Second, recognizing the rapidly developing nature of the Internet, Congress sought to protect continued innovation and creativity in enacting Section 230. That innovation has allowed for the Internet to scale to carry previously unimaginable amounts of information and utility—which would not be possible without technologies like algorithms. Grafting an atextual “traditional editorial functions” limitation onto the statute would severely undermine the Internet’s innovative benefits.

Third, Section 230 immunity is crucial to the continued flourishing of the Internet ecosystem as it has

developed. The infrastructure of the Internet consists of different layers in a “stack,” which include multiple intermediaries transmitting third-party content. The current Section 230 regime has protected this infrastructure by (a) creating certainty and predictability for a broad range of Internet providers and (b) ensuring that the responsibility for content published online lies with the content-creator, not the wide diversity of Internet service providers that facilitate the transmission and delivery of the content. Section 230 immunity also benefits a wide range of Internet participants at many levels of the Internet stack, from bloggers across the political spectrum to small businesses to cybersecurity firms to large “user generated content” platforms. Any erosion of Section 230 protections would undermine the intent of Congress, and many individuals and entities—far beyond large tech companies or social media platforms—would be harmed.

This Court should affirm.

◆

ARGUMENT

Congress enacted Section 230 to protect and encourage the interactive nature of the Internet, to foster its growth and innovation, and to protect providers’ ability to allow—or block—content on the Internet. The plain language of Section 230 fosters both the unique ability for participants to communicate that is a foundational feature of the Internet *and* provides broad protection for invention in an unknown but

creative future. It says nothing about “traditional editorial functions,” and the Court should not graft such a limitation onto the statute. Section 230 works—and the Internet as we know it depends on it.

I. Through Section 230, Congress Expressly Sought to Protect and Enable a Medium for Unique Modes of Interactivity.

One of Congress’s explicit goals for Section 230 was “to promote the continued development of the Internet and other interactive computer services and other interactive media.” 47 U.S.C. 230(b)(1). Congress recognized that interactive computer services in general, and the Internet in particular—even at its early stage when Section 230 was enacted—offered what was at the time a profoundly unique platform for interactive communication. Congress observed in the statute that 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.” *Id.* 230(a)(3). In Congress’s judgment, these interactive communications, which foster public discourse, should be encouraged.

The Internet, unlike prior “published” forms of mass communication, transforms the individual from a passive user into an active participant in shaping communication and content. Individuals have new ways to speak to and engage with one another, with unprecedented scope and scale, able to connect,

collaborate, and debate with people across town or around the world. Congress recognized that this interactivity was an essential attribute of the emerging Internet that warranted protection.

A. Interactivity Has Been Key to Online Communications Since Before the Internet Became a Publicly Available Resource.

Section 230 was enacted in 1996, near the beginning of the public use of the Internet, and provided essential protections for interactivity in response to critical court decisions and associated uncertainty that had emerged in the early days of online communications.

The Internet was developed in the 1970s within the U.S. academic community through a U.S. federal government project.² Even at this early stage, the potential for interactivity unique to the Internet was plain. In the 1970s and 1980s, it was used primarily for collaboration between academic, government, and commercial researchers, with non-research commercial traffic effectively prohibited. At the same time, private networks were created, ranging from commercial-focused communications networks to “bulletin board” services for individuals or small groups to communicate. One of the earliest successful private networks—

² Vint Cerf, *A Brief History of the Internet and Related Networks*, Internet Society, <https://www.internetsociety.org/internet/history-internet/brief-history-internet-related-networks/>.

CompuServe—was founded in 1969 as a “dial up” network aimed at businesses, before broadening its services to include individuals, who were then able to engage, share content, and collaborate with people far beyond their local communities. Ultimately, the Internet itself transitioned to be a privately owned and operated network in April 1995, about nine months before Section 230 was enacted.³

As the Internet evolved and expanded—and more and more individuals joined the growing global conversation—debates emerged about the legal responsibility for online content on these new communications platforms, particularly with respect to the novel outlets allowing interactivity and public dialogue.

In the 1990s, two seminal cases addressed online service providers’ liability. *Cubby, Inc.* held that an online service provider could not be held liable for speech made by a participant in an online forum because the provider had not regulated any content. *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991). Then *Stratton Oakmont, Inc.* held an online service provider liable for participants’ speech because the provider engaged in some content monitoring and regulation. See *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). These cases created significant uncertainty and potentially crippling liability for the newly

³ See *A Brief History of NSF and the Internet*, National Science Foundation (Aug. 13, 2003), https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.

developing industry of online service providers, including companies that facilitated access to the Internet and third-party speech.

It is against this backdrop that Congress considered and enacted the “Internet Freedom and Family Empowerment Act,” which became Section 230.⁴

B. Congress Protected the Interactivity of the Internet with Section 230.

Through the “Internet Freedom and Family Empowerment Act,” which became Section 230, Congress sought to protect Internet service and content providers from liability for third-party content, and to empower those providers to block objectionable content without risk of liability.

Fundamentally, Congress sought to foster this platform for communication and connection, to enable

⁴ The “Internet Freedom and Family Empowerment Act” passed by the U.S. House of Representatives in part as an alternative to the “Communications Decency Act” (CDA), which was proposed and passed in the U.S. Senate. A joint Senate-House conference committee decided to include both the CDA and House-passed Section 230 in the Telecommunications Act of 1996. The CDA’s rules on “indecent” and “patently offensive” content were quickly challenged and subsequently struck down on First Amendment grounds by this Court in *Reno v. ACLU*, 521 U.S. 844 (1997), but Section 230 had not been challenged and was not at issue in the *Reno* decision. See Ashley Johnson & Daniel Castro, *Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved*, ITIF (Feb. 22, 2021), <https://itif.org/publications/2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved>.

new mediums for interactive dialogue. See, e.g., 47 U.S.C. 230(b)(1). Prior to the rise of the Internet, broadcast and video media consisted almost entirely of services that conveyed to a passive audience content published by large media companies. The Internet was not simply a cable service with far more channels, but a wholly new medium in which individuals could be content creators and publishers.

The Internet allows participants access to a vast “free market” of resources and information, including the ability to “control” what information is received, and, most novelly, to participate in shaping communication and content through individuals creating and publishing their own content. See *id.* 230(a), (b)(2)-(3). To accomplish these interactivity goals, Congress enacted a law that upended traditional publisher liability and made clear that Internet service and content providers would not be liable for content posted by other online participants.

The results are undeniable. A vast amount of communication (artistic, political, intellectual, pedestrian, and otherwise) now flows through the Internet—whether through blogs, message boards, social media both large and small, videos or music uploaded to the Internet, or other means. The “dramatic expansion of this new marketplace of ideas” has only continued since this Court’s decision in *Reno v. American Civil Liberties Union*, 521 U.S. 844, 885 (1997). See also *Am. Civil Liberties Union v. Reno*, 929 F. Supp. 824, 881 (E.D. Pa. 1996) (observing the beneficial “democratizing” effects of Internet interactivity and noting “that

the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country—and indeed the world—has yet seen”). This Court should uphold Section 230 protections and the resulting interactivity that is fundamental to the Internet today.

II. Far from Enshrining a “Traditional” Concept of Communications Regulation, Section 230 Created a Framework to Support the Internet’s Innovation.

Nothing in the text of Section 230 calls for interactive computer services to be treated the same as traditional publications like newspapers or book editors. That makes sense. Editorial functions vary tremendously depending on the medium and how participants engage with the forum. And the Internet was and is a wholly new and different way for content to be created, distributed, and consumed.

A. Section 230 Fosters Editorial Innovation.

As Congress stated, the Internet and other interactive computer services were “rapidly developing,” 47 U.S.C. 230(a)(1)—and they continue to rapidly develop. Adopting an interpretation that protects only “traditional” editorial functions would threaten modern Internet developments and *restrict* the Internet’s growth

and development—exactly what Congress sought to avoid.⁵

⁵ Many on both the right and the left of the political spectrum in the United States have responded to certain innovations by arguing for changes to, or even repeal of, Section 230, and Members of Congress have introduced a broad range of bills that would impact Section 230. See, e.g., Amicus Br. of Ted Cruz, et al., at 1 (referring to Republican congressmembers’ proposed “legislation to revise or repeal § 230”); Press Release, House Committee on Energy & Commerce, E&C Leaders Announce Legislation to reform Section 230 (Oct. 14, 2021), <https://energycommerce.house.gov/newsroom/press-releases/ec-leaders-announce-legislation-to-reform-section-230> (proposed legislation to revise Section 230 from Democratic congressional leaders); Joe Biden, *Republicans and Democrats, United Against Big Tech Abuses*, WSJ Opinion (Jan. 11, 2023), <https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrust-children-algorithm-11673439411>. Many critiques of Section 230, however, have urged diametrically opposing changes to the statute; some advocate that “more” moderation of content and speakers should be required, while others have urged that “less” moderation of content and speakers is necessary. See Chris Riley & David Morar, *Legislative efforts and policy frameworks within the Section 230 debate*, Brookings (Sept. 21, 2021), <https://www.brookings.edu/techstream/legislative-efforts-and-policy-frameworks-within-the-section-230-debate/>. And at the same time, some Congressional proposals have drawn bi-partisan support—but also have encountered bi-partisan opposition. In light of this broad disagreement within Congress on how, if at all, Section 230 should be altered—and the resulting legislative inaction to date—this Court should be particularly hesitant to alter the Section 230 regime, and should leave these policy decisions to the legislative branch where they belong. See, e.g., *Nat’l Fed’n of Indep. Bus. v. Sebelius*, 567 U.S. 519, 538 (2012) (“Members of this Court are vested with the authority to interpret the law; we possess neither the expertise nor the prerogative to make policy judgments. Those decisions are entrusted to our Nation’s elected leaders, who can be thrown out of office if the people disagree with them.”).

In seeking to protect innovation, Congress expressly anticipated that many “editorial functions”—including “filter[ing], screen[ing], allow[ing], * * * disallow[ing,] * * * choos[ing] * * * organiz[ing], reorgan[izing] or translat[ing] content”—would be *performed by computer software*, not by humans. See 47 U.S.C. 230(c)(2)(B), (f)(4). Congress also anticipated—and supported—the use of computer software to filter content on the Internet. This express embrace by Congress of non-traditional tools to organize content belies any assertion that Section 230 is limited to “traditional” editorial functions.

The sheer volume of content shared on the Internet has prompted an increasing reliance on algorithms that automatically sort and display content, and, for advertising-supported platforms, to algorithms that select and display advertisements alongside content. It would be impossible for a website owner with tens of thousands of hours of videos uploaded to the site every day to engage in the same function as a traditional newspaper editor. Algorithms are necessary to sort that information. A website owner should not be held liable for third-party content simply because technology has advanced to facilitate vast content sharing.

Algorithms are now essential to the normal function and use of a wide variety of websites. Algorithms

search for erroneous⁶ or malicious content.⁷ Algorithms improve e-commerce websites and direct desired content on social media platforms. Algorithms also are vital for increasing accessibility, as algorithms convert voice into text captions for hard of hearing and deaf individuals.

Further, Section 230 facilitates editorial innovation by lowering the cost to enter the field. A small start-up may not need to hire attorneys to determine liability risks before it can open its virtual doors on the Internet. Instead, that start-up can invest in engineering, technological advancements, and improvements to participant experience. And it need not fear the imposition of liability merely based on that innovation itself.

B. Section 230 Does Not Include a “Traditional Editorial Function” Standard.

This Court should not impose a new “traditional editorial function” standard, but should affirm the standard applied by the Ninth Circuit majority in this case—the language of the statute itself: “Section

⁶ See, e.g., EarthData, *Data Tools* (Oct. 29, 2020), <https://www.earthdata.nasa.gov/learn/use-data/tools>; Saurav Mohapatra, *MaRS: How Facebook keeps maps current and accurate*, Engineering at Meta (Sept. 30, 2019), <https://engineering.fb.com/2019/09/30/ml-applications/mars>.

⁷ See, e.g., Analytics Insight, *Wikipedia employs AI to learn more about the issue its facing and consider possible solutions*, Swiss Cognitive (June 10, 2021), <https://swisscognitive.ch/2021/06/10/wikipedia-and-ai>.

230(c)(1) precludes liability for ‘(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat * * * as a publisher or speaker (3) of information provided by another information content provider.’” *Gonzalez v. Google LLC*, 2 F.4th 871, 891 (9th Cir. 2021) (quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100–01 (9th Cir. 2009)). The statute imposes just those three factors.

The Ninth Circuit standard has the advantage of tracking the congressional language and establishing a clear line for liability protection. By contrast, a “traditional editorial” standard is not found in the text of the statute, and it would be a nebulous and subjective standard open to varying interpretations. An algorithm used by a video site that prioritizes the videos most likely to be consumed by an individual, based on the individual’s previous selections, does not engage in a “*traditional* editorial function” because it is curated to each individual, does not involve human selection, and may consider a broad range of factors beyond newsworthiness. Crucially, however, none of these factors are relevant under the statute. This Court should make clear that whether an activity is “traditionally” editorial, or rather depends on innovative technology to the benefit of Internet participants, is irrelevant.⁸

⁸ This analysis does not in any way suggest that the discussion of “traditional editorial functions” in the seminal decision in *Zeran v. Am. Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998), was incorrect. Section 230 clearly provides liability protection for those editorial functions at issue in *Zeran*. But as numerous lower court cases have found in the 25

Congress could not have predicted how and the degree to which the Internet would evolve. But, with Section 230, Congress intentionally facilitated that future innovation. Pigeonholing Section 230 to newspaper-like websites would undercut Congress's intention.

III. Section 230 Immunity Is Crucial to the Flourishing of Many Different Parts of the Internet Ecosystem.

The Court should give due consideration to Section 230's impact in allowing the Internet to welcome and support the interactive contribution and access—whether blog posts, videos, music, graphic art, anything—by hundreds of millions of people a day in the United States alone, and the severe risks to that individual participation that are likely to follow from a misreading of the law.

A. Section 230 Protection Is Essential.

1. The Internet's infrastructure

The Internet today is a complex, interconnected network of networks. Around the world, there are thousands of interconnected networks operated by different service providers, companies, universities, local communities and governments, with no single entity in control of the whole. Understanding how the Internet functions, the different entities involved in its

years since *Zeran*, Section 230 *also* protects a broad range of “non-traditional” editorial and content management functions.

functioning, and the indispensable role of algorithms is essential here.

First, the Internet consists of non-proprietary reusable “building blocks” of technologies and protocols that are assembled in an “open” and easily upgradable architecture used by different entities—sometimes referred to as “intermediaries”—in different ways to maintain the networks, transmit data, and provide access to the transmitted content. The Internet is decentralized—each of those thousands of networks “makes independent decisions on how to route traffic to its neighbors, based on its own needs, business model, and local requirements.”⁹

The architecture of the Internet is generally described as a layered stack. In the bottom layer of the stack—the link layer—physical connections are provided to participants’ computers.¹⁰ These can be wired installations, such as copper, coaxial or fiber-optic

⁹ Internet Society, *Internet Way of Networking Use Case: Intermediary Liability* (Sept. 9, 2020), <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-intermediary-liability/>.

¹⁰ See Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME LAW REV. 815, 816 (2004). The “layers” model is a helpful explanatory framework with which to understand the differing technical roles and functions that make the Internet possible. The reality is not always as crisp and well defined as the theory, in that, for example, in some circumstances some layer functions could be implemented at another layer. The analytical model is nevertheless useful to understand how characters typed on a keyboard can get bundled into “packets,” transmitted around the world, reassembled at the destination, and then displayed on a distant screen.

cable, or can be wireless. On top of this layer is the network layer (or “Internet Protocol” layer), at which ISPs deliver so-called IP packets and collectively provide an abstract global network: the Internet.¹¹ Above the network layer is the application layer,¹² utilized by a huge diversity of services and applications ranging from familiar tools used by people to machine-to-machine communications (such as a security system checking in with a monitoring service) to “Internet of Things” devices communicating with each other and controlling systems in the real world. People-focused applications that use Internet connections include e-mail, web browsing, social media offerings, automatic photo backups, and audio and movie streaming, among many others. This layer then displays or delivers the content—the images, words and symbols being communicated.¹³

Different players are responsible for managing elements at different layers. An infrastructure provider might offer a fiber connection to an office. The office might engage in a contract with an ISP to provide an Internet service over the fiber. And they may engage

¹¹ *Ibid.*

¹² Technically, there is the transportation layer between the network and application layer, where perceptions of connections between computers are created. The transportation layer is implemented on all computers connected to the Internet. *Ibid.* The transportation layer is not relevant to the focus of this brief.

¹³ *Ibid.* For additional discussion of the Internet’s stack or layers, see also *The TCP/IP stack*, Isaac Computer Science, https://isaacomputerscience.org/concepts/net_internet_tcp_ip_stack?examBoard=all&stage=all.

with many vendors to supply email, Internet telephony, video conferencing, and business services. It is important to keep in mind, however, that the layers in practice are interdependent, so interventions at one layer of the stack likely will have consequences for other layers. And all these types of providers are “interactive computer service” providers protected by Section 230. 47 U.S.C. 230(c)(2). Without Section 230, service providers at many levels could be at risk of legal attacks for allowing undesired content to cross through their networks.

Intermediaries serve varying roles depending on where they operate within the Internet “stack.” Intermediaries operating at different layers will have a different relationship “to data and knowledge of its content.”¹⁴ Intermediaries at the application layer (e.g., websites and social media platforms) have a greater potential knowledge of the data’s content¹⁵ used by the application they provide than intermediaries at the network layer (e.g., content delivery

¹⁴ Internet Society, *Internet Way of Networking Use Case: Intermediary Liability* (Sept. 9, 2020), <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-intermediary-liability/>. This distribution of responsibilities also gives rise to the end-to-end principle, which recognizes that “intelligence in the network resides at the ends or in the applications.” *Id.* Some intermediaries may operate at multiple levels of the stack because they offer different types of services—for example, ISPs that also offer email services.

¹⁵ It is not certain, however, that even these application layer intermediaries would have knowledge of the content, given the development of end-to-end encryption which scrambles the data so that it is not visible for any intermediary in the stack.

networks, Internet service providers, and domain name registries), which serve a specific infrastructure purpose that may not need or even be able to know what is flowing through the Internet's pipes and over their own networks.¹⁶

Today, there are billions of Internet participants depending on this infrastructure to access, create, and share vast quantities of data, content, and information. The sheer volume of data makes the maintenance of networks and transmission of that data impossible without algorithms. At the network layer (where networks exchange Internet traffic), routing algorithms are used to decide the path on which the packets are sent based on data about load, latency, and other factors, a task completely impossible to maintain without algorithms making decisions about what content must go where to make it to its destination. And at the application level, given the complexity and volume of shared content and information, algorithms are often used to screen out unsafe content for minors, improve search results, and even keep spam e-mails out of inboxes. The use of algorithms is pervasive throughout the operation of the Internet, and a decision that algorithmic processing is unprotected by Section 230 would be devastating at the application layer, and would increase risk and uncertainty at other layers.

¹⁶ *Internet Way of Networking Use Case: Intermediary Liability, supra.*

2. The importance of intermediary immunity

The existing intermediary liability protection scheme, facilitated by Section 230, shields interactive computer services from liability for third-party content. This protection, along with the intermediary immunity regimes it has inspired in other influential countries,¹⁷ has been critical for the Internet's development and is essential for the Internet to continue to flourish.

The current regulatory regime has (1) created certainty and predictability for a broad range of types of Internet providers and (2) ensured that the burden of what content will be published and how depends on the content-creator, not the Internet provider.¹⁸

Section 230 has also paved the way for permission-less innovation and permission-less content offerings. Taking the example of video content, in the media networks that pre-dated the Internet, a new content provider (say, a new cable channel) had to arduously negotiate with many different cable systems to allow their new content to be delivered and to agree on negotiated liability assignments to cover the delivery of the content. On the Internet—because of Section 230—

¹⁷ See World Intermediary Liability Map, <https://wilmap.stanford.edu>, for a helpful catalogue of intermediary liability laws around the world.

¹⁸ *Intermediary Liability: The Hidden Gem*, Internet Society (Mar. 11, 2020), <https://www.internetsociety.org/blog/2020/03/intermediary-liability-the-hidden-gem>.

anyone can start a website to share a video they made without any negotiation with anyone else beyond an agreement to obtain access to the Internet. If any Internet participant has a new idea for an online service, they can develop it and make it available and, if people like it, the new service can succeed. Indeed, almost all major online social media and video platforms today started in exactly that manner—in an innovator’s proverbial garage.

Section 230’s protection from potential liability has been essential in fostering these and many other technologies, integral to the Internet as it exists today, and the modern economy at large.¹⁹

B. Section 230 Protection Is Crucial to a Wide Range of Providers and Companies at Many Levels of the Stack.

Section 230 offers vital protection at each layer of the Internet stack—not just the application or interface layer. For example:

Internet Service Providers (“ISPs”) make it possible for individuals to access the Internet. Whether through cable, digital subscriber lines, fiber, or satellite connections, ISPs enable Internet access. Section 230 ensures that ISPs are not responsible for regulation and monitoring of third-party content for these

¹⁹ See, e.g., David Belson, *Is the Internet Resilient enough to Withstand Coronavirus?*, Internet Society (Feb. 28, 2020), <https://www.internetsociety.org/blog/2020/02/is-the-internet-resilient-enough-to-withstand-coronavirus>.

services.²⁰ Any responsibility for third-party content, or requirement to review third-party content, likely would grind ISPs to a halt and freeze the Internet as we know it. ISPs carry enormous quantities of traffic every second, in a huge array of formats and applications, most of which is encrypted for security. ISPs cannot feasibly assess all network layer packets' content for potential liability. Requiring as much would be analogous to a courier needing to intercept thousands of letters between many people in many different languages, translate the content, and then ensure against potential liability. This is infeasible and would be a significant barrier to entry.

Content Delivery Networks (CDNs), which are specialized network providers, also depend on Section 230 immunity. CDNs are geographically distributed networks of proxy servers and data centers, and they are crucial to delivering large amounts of data (such as delivering high-definition streaming video) quickly to many viewers simultaneously. CDNs incorporate algorithms to decide what content to store where, depending on local demand, and to ensure content is distributed for quick and reliable delivery. They are dedicated to providing fast, low-latency content, and are an example of beneficial Internet network innovation made possible by Section 230. CDNs use Internet functionality—e.g., “anycast” routing—to route data

²⁰ Section 230(d) requires ISPs to notify customers that filtering services (such as cleaninternet, cleanbrowsing, and cleanrouter) are available to limit minors' access to certain materials.

packets to popular destinations and ensure that content and communications are quickly delivered. CDNs also often screen for cyber security concerns.

And at the level of the stack perhaps most familiar to the end-user, software on computers may include anti-virus and anti-malware protections. Providers of that software likewise rely on Section 230 protections for immunity regarding screening and blocking offensive material. See *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1177–78 (9th Cir. 2009) (“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.”). This is exactly the sort of innovation Section 230 anticipated and encourages. See 47 U.S.C. 230(c)(2)(B), (f)(4) (protecting providers of software or tools that “filter, screen, allow, or disallow content”).

Narrowly reading Section 230 could require any or all of these entities—at any level of the stack—to institute changes that would make it impossible to continue providing certain services and critical Internet security features.²¹ Infrastructure intermediaries that route traffic around the Internet could—because of

²¹ Internet Society, *Internet Way of Networking Use Case: Intermediary Liability* (Sept. 9, 2020), <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-intermediary-liability/>.

liability concerns in the absence of Section 230 or if Section 230 is altered in any way—decide that they must alter their current approach to routing and make routing policy based on the potential content of information in ways that would bog down traffic flow. If the use of algorithms to distribute third-party content opens one up to liability, that may upend the feasibility of individual networks collaborating with other networks on a global scale without incurring significant costs, such that networks are no longer focused on efficiency and speed at the packet level (based on factors like size, destination, and volume), but are focused on liability risk. That likely would lead to a splintering of the Internet, such that certain parts of the network would not be accessible to other parts of the network.²²

Any changes to Section 230 immunity could have unintended consequences given the complex and varying roles different intermediaries play in the Internet infrastructure. In order to continue to protect the Internet as we know it, the Court must preserve intermediary immunity.

C. Section 230 Protection Is Vital for Individuals, Small Companies, and Non-profits.

Weakening intermediary immunity would harm individuals, small companies, and not-for-profit organizations. Section 230 allows small companies to flourish without fear of crippling legal liability. Some small

²² See *ibid.*

online retailers allow individuals to comment or post reviews in order to compete with larger retail platforms; other small retailers rely on third-party search engines embedded on their website; resources like Wikipedia.org provide community-generated information on a litany of topics; and advocacy organizations utilize the Internet to empower vulnerable communities to communicate and learn from each other. Section 230 protection allows these different companies and groups to fully embrace the global connectivity of the Internet.

Section 230 is also crucial for a wide range of online communities. Section 230 immunity protects blog-based content that allows commenting, like blogger.com (and individuals or organizations that create blogs through this platform) or websites allowing for topic-based content like Alltrails.com—a well-known source for hikers to share information and advice on hiking trails. Other platforms like GitHub²³ and GitLab²⁴ allow distribution of open source computer code and collaboration. Such forums for communication can only remain as they are so long as the forum itself remains free from liability, even if it uses algorithms or other technologies to display content.²⁵

²³ See <https://github.com/>.

²⁴ See <https://about.gitlab.com/>.

²⁵ In this way, intermediary immunity protects all sorts of democratic dialogue, including both right-of-center and left-of-center blogs, which rely on this type of protection.

Altering Section 230 immunity could be devastating for individuals, small businesses, non-profits, and online communities, which likely lack the resources to monitor and regulate participant-created content. If intermediaries become subject to liability, the Internet may become a web of complex liability-shifting regimes, which could make sharing content prohibitively expensive, ultimately stifling the citizen speech Congress sought to foster. 47 U.S.C. 230(a)(3). The Internet has flourished with Section 230 intermediary immunity, and it should be protected.

◆

CONCLUSION

For these reasons, the Internet Society respectfully requests that this Court affirm the Ninth Circuit. At a minimum, the Internet Society respectfully requests that the Court hold that Section 230 is not limited to “traditional editorial functions” and continues to protect all kinds of activities involving third-party content.

Respectfully submitted,

RAEHEL KEAY KUMMER

Counsel of Record

JAMES D. NELSON

MEREDITH L. COMPTON

MORGAN, LEWIS & BOCKIUS LLP

1111 Pennsylvania Avenue, N.W.

Washington, DC 20004

(202) 739-3000

raechel.kummer@morganlewis.com

JANUARY 2023