24-2386

United States Court of Appeals for the Second Circuit

UNITED STATES OF AMERICA,
Plaintiff-Appellant,

v.

EZ LYNK, SEZC, PRESTIGE WORLDWIDE SEZC, THOMAS WOOD, BRADLEY GINTZ,
Defendants-Appellees.

On Appeal from the United States District Court
for the South District of New York

BRIEF OF *AMICI CURIAE* CHAMBER OF PROGRESS, COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION, CONSUMER TECHNOLOGY ASSOCIATION, ELECTRONIC FRONTIER FOUNDATION, ENGINE ADVOCACY, AND NETCHOICE IN SUPPORT OF APPELLEES AND AFFIRMANCE

Brian M. Willen
Wilson Sonsini Goodrich & Rosati, P.C.
1301 Ave. of the Americas, 40th Floor
New York, NY 10019
(212) 999-5800
bwillen@wsgr.com

Lauren Gallo White
Wilson Sonsini Goodrich & Rosati, P.C.
One Market Plaza, Spear Tower, Ste 3300
San Francisco, CA 94105
(415) 947-2000
lwhite@wsgr.com

Paul N. Harold
Steffen N. Johnson
Wilson Sonsini Goodrich & Rosati, P.C.
1700 K Street, N.W.
Washington, D.C. 20004
(202) 973-8800
pharold@wsgr.com
sjohnson@wsgr.com

Counsel for Amici Curiae

RULE 26.1 CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Civil Procedure, *Amici Curiae* Chamber of Progress, Computer & Communications Industry Association, Consumer Technology Association, Electronic Frontier Foundation, Engine Advocacy, and NetChoice each state that they have no parent corporation and that no publicly held corporation owns 10% or more of their stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTERESTS OF *AMICI CURIAE*[1]

Chamber of Progress is a tech-industry coalition devoted to a progressive society, economy, workforce, and consumer climate. Chamber of Progress backs public policies that will build a fairer, more inclusive country in which the tech industry operates responsibly and fairly, and in which all people benefit from technological leaps. Chamber of Progress seeks to protect Internet freedom and free speech, promote innovation and economic growth, and empower technology customers and users. Chamber of Progress's work is supported by its corporate partners, but its partners do not sit on its board of directors and do not have a vote on, or veto over, its positions. Chamber of Progress does not speak for individual partner companies, and it remains true to its stated principles even when its partners disagree.

The **Computer & Communications Industry Association** ("CCIA") is an international, not-for-profit trade association representing a broad cross section of communications, technology, and Internet industry firms that collectively employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global

[1] No party's counsel authored this brief in whole or in part. No party or party's counsel contributed money that was intended to fund preparing or submitting this brief. No person, other than the *amici curiae*, their members, or their counsel, contributed money that was intended to fund preparing or submitting this brief. All parties have consented to the filing of this brief.

economy. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA believes that open, competitive markets and original, independent, and free speech foster innovation. A list of CCIA members is available at www.ccianet.org/members.

The **Consumer Technology Association** ("CTA") represents the $505 billion U.S. consumer technology industry, which supports more than 18 million U.S. jobs. CTA's membership is over 1,300 American companies—80% of which are small businesses and startups. CTA also owns and produces CES®, the world's most powerful technology event.

The **Electronic Frontier Foundation** ("EFF") is a member-supported, nonprofit civil liberties organization that has worked for more than 30 years to protect innovation, free expression, and civil liberties in the digital world. On behalf of its more than 30,000 dues-paying members, EFF seeks to ensure that the interests of its members and other users who rely on internet platforms are represented in courts considering crucial online free speech issues, including the right to transmit and receive information online.

EFF has litigated or otherwise participated in a broad range of internet free expression and intermediary liability cases because such cases often raise novel issues surrounding free expression and the rights of internet users. EFF often files amicus curiae briefs in these cases because their outcome can significantly impact,

and sometimes curtail, the free expression rights of individuals who rely on internet platforms. *See, e.g.*, *Packingham v. North Carolina*, 582 U.S. 98, 104 (2017) (citing EFF's *amicus curiae* brief). EFF believes that 47 U.S.C. § 230 ("Section 230") is a foundational law that enables internet speech by protecting the intermediaries that host people's speech. EFF thus regularly participates in cases that seek to limit Section 230 because such limitations jeopardize users' free speech.

Engine Advocacy ("Engine") is a non-profit technology policy, research, and advocacy organization dedicated to bridging the gap between startups and policymakers. Engine works with government officials and a community of thousands of high-technology, growth-oriented startups across the nation to support innovation and entrepreneurship through research, policy analysis, and advocacy. Engine's community of startups includes small- and medium-sized companies that host user-generated content. Engine and its community of entrepreneurs and supporters seek to protect the opportunities that exist for startups and their users thanks to the robust protections provided by Section 230.

NetChoice is a national trade association of e-commerce and online businesses that share the goal of promoting convenience, choice, and commerce on the Internet. For over a decade, NetChoice has worked to increase consumer access and options via the Internet, while minimizing burdens on small businesses that are making the Internet more accessible and useful.

Amici share an interest in the proper interpretation and application of 47 U.S.C. § 230's protections for all online services. Those protections are critical to ensuring the free flow of information online and the flourishing of the Internet.

INTRODUCTION AND SUMMARY OF ARGUMENT

Section 230 represents Congress's policy choice to ensure that the Internet remains a robust forum for information, services, and commerce—and that claims arising from allegedly unlawful material be directed at those who originate such material, rather than those who provide a platform for its dissemination. *See Force v. Facebook, Inc.*, 934 F.3d 53, 63 (2d Cir. 2019) (quoting 47 U.S.C. § 230(b)). The flourishing of the modern Internet is made possible by Internet intermediaries, which host all kinds of third-party information, from social media posts, videos, and photos, to apps and other digital tools made of computer code, not unlike EZ Lynk here. The government's case against EZ Lynk depends on imposing liability for third-party content made available by an "interactive computer service" and therefore runs headlong into Congress's decision to shield such services from the burdens of litigation and liability for third-party content.

Seeking to avoid this bedrock protection, the government invites this Court to depart from the statute text and purpose—and come into direct conflict with other Circuits. The government's arguments threaten serious consequences for the entire Internet ecosystem. Accepting them would chill the availability of diverse and open

platforms that permit Internet users to share a variety of speech online, including computer code.

First, the government contends that Section 230 protects interactive computer services only when they are disseminating information "for a human audience." Gov't Br. 25. Under that atextual and amorphous interpretation, any service that disseminates third-party code—from mobile app stores, to cloud storage, to web hosting services, to open-source code repositories and collaboration platforms—could potentially face liability for claims based on the code's function. That would leave unprotected the vast oceans of computer code that underpin the Internet and modern computing, including all the code that makes communicating speech over the Internet possible. In particular, the government's approach would also pose an existential risk to app stores, which host millions of third-party software programs that users download and run on their devices. App stores and other important online services would rationally respond by restricting the information they disseminate, shrinking or shuttering the very "forum[s]" for "discourse" and "intellectual activity" that Congress intended Section 230 to foster. 47 U.S.C. § 230(a)(3).

Fortunately for the Internet and everyone who uses it, Section 230's text, purpose, and persuasive precedent foreclose the government's argument. The ordinary meaning of information is broad, encompassing all forms of data. And Section 230 applies to "*any* information," 47 U.S.C. § 230(c)(1) (emphasis added),

underscoring that the statute is agnostic to the form of information that third-parties disseminate via interactive computer services. This text readily encompasses software like the tunes at issue here. Indeed, while the government inexplicably ignores it, the Third Circuit has expressly held that the "information" protected by Section 230 includes harmful and illegal computer software programs. *Green v. Am. Online (AOL)*, 318 F.3d 465, 471 (3d Cir. 2003) (Section 230 bar claims against interactive computer service provider for allegedly disseminating malware created by a third party). Accepting the government's flawed argument would create an unwarranted circuit split, which is reason alone to reject it.

Second, the government contends that its claim does not "treat" Defendants as "publisher[s]" of third-party information, 47 U.S.C. § 230(c)(1), in large part because the EZ Lynk System includes a "hardware" component, Gov't Br. 2, 22, 24, 31. But, properly understood, the alleged conduct "falls within the heartland of what it means to be the 'publisher' of information under Section 230(c)(1)." *Force*, 934 F.3d at 65. The crux of the government's claim is that the EZ Lynk System makes available software programs developed and uploaded by third parties through the EZ Lynk Cloud. That allegation targets core publishing conduct. The fact that the EZ Lynk System includes a hardware *component* changes neither the fact that the system functions to deliver third-party information nor that the claim treats Defendants as the publishers of the third-party delete tunes. Any holding that a defendant loses

Section 230 protection by providing hardware "tools to access [third-party] software," Gov't Br. 33, would strike at the roots of the Internet ecosystem.[2]

Finally, the government argues that the district court was "particularly" "wrong" to dismiss its Clean Air Act claim based on Section 230 as an "affirmative defense." Gov't Br. 3. But there is nothing wrong or even unusual in dismissing a claim barred by Section 230 at the pleading stage, where, as here, its application is evident from the face of the complaint. *See* JA-119. This Court has done so repeatedly, and courts across the country do so routinely. The district court's approach below followed this precedent and widespread practice. Screening out cases clearly barred by Section 230 at the motion-to-dismiss stage furthers Congress's purposes to the benefit of interactive computer services, their users, and the public. By reducing the spectre of litigation costs, the practice of early Section 230 rulings blunts the risk that litigation can be used as a heckler's veto to silence speech by imposing hefty litigation costs on forums for information. This Court should reaffirm that "application of Section 230(c)(1) is appropriate at the pleading stage." *Force*, 934 F.3d at 63 n.15.

[2] Of course, the mere fact that a hardware device can be used for unlawful purposes, does not itself make the device unlawful. *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984) (holding that the Sony Betamax recorder was capable of substantial noninfringing uses and therefore the sale of the recorder did not give rise to liability for contributory copyright infringement).

ARGUMENT

I. The Court Should Reject The Government's Argument For A "Software Code" Exception To Section 230.

The government asserts that Section 230 has no place in this litigation and leads with the argument that Section 230 protects interactive computer services only when they are disseminating "information" "for a human audience," not software. Gov't Br. 25. Statutory text, purpose, and persuasive authority all point to the contrary: Section 230's protections apply to information of whatever kind, including computer code. The government's argument is not only wrong, it is dangerous. Carving out computer code from Section 230's ambit would risk severe disruptions to the Internet ecosystem, ultimately chilling speech and making the Internet less useful and vibrant.

A. Text and precedent establish that Section 230 applies to "any information" of whatever kind, including computer code.

Section 230's protections are not limited to human speech; instead, the statute uses the broader term "information," which carries its "ordinary meaning." *BP P.L.C. v. Mayor & City Council of Baltimore*, 593 U.S. 230, 237 (2021); *accord Force*, 934 F.3d at 65 (looking to "ordinary meaning" when interpreting the undefined term "publisher" in Section 230). The ordinary meaning of "information" is broad. It includes all forms of "data" and the "signal[s] or character[s] … representing data." *See Merriam-Webster's Collegiate Dictionary* 599 (1996)

("FACTS, DATA"; "a signal or character (as in a communication system or computer) representing data"). What is more, the statutory phrase "*any* information" underscores that Section 230's protections encompass information "'of whatever kind.'" *See Ali v. Fed. Bureau of Prisons*, 552 U.S. 214, 219 (2008) ("[R]ead naturally, the word 'any' has an expansive meaning, that is, 'one or some indiscriminately of whatever kind.'"). To the extent any ambiguity remains, the courts of appeal agree that "the text of Section 230(c)(1) should be construed broadly in favor of immunity." *Force*, 934 F.3d at 64 (collecting cases).

As the Third Circuit has held, the ordinary meaning of "information" under Section 230(c)(1) easily encompasses computer code like the tunes at issue here. *See Green*, 318 F.3d at 471 (noting that under the dictionary meaning of "information," the term included a hacker's computer signal and software program used to shut down a computer). It plainly encompasses the information that the government says its claim targets here—"computerized commands for disabling a vehicle's emission controls," Gov't Br. 25—because these are "data" and "signal[s]." *Merriam-Webster's Collegiate Dictionary* 599 (1996); *see* JA-26 ¶ 48 ("Once the Auto Agent is connected to the EZ Lynk Cloud through the Auto Agent App, drivers are able to send and receive data and software relating to their vehicles' computer systems."). Indeed, the government itself defines "tune[s]" as "information." *See* JA-62 (Environmental Protection Agency's Information

Requests to Defendants) (defining "tune" as "any combination of software programming, calculations, computer logic, tables of information (*e.g.*, fuel timing maps), coding, or other content or information, stored in any form, capable of affecting or controlling an electronic control module").

Statutory context confirms the breadth of the ordinary meaning of "information." Section 230 protects providers of "interactive computer service[s]," 47 U.S.C. § 230(c)(1), which include "any information service[] … that provides or enables computer access by multiple users to a computer server," 47 U.S.C. § 230(f)(2). "Information service" is in turn defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." 47 U.S.C. § 153(24). As these definitions show, Section 230's protections are not limited to online providers who merely display the narrow subset of information intended to be seen by humans; rather, a provider qualifies for Section 230's protections whenever it "stor[es]" or "utiliz[es]" or "mak[es] available" information of any kind. 47 U.S.C. § 153(24). Consistent with this broad definition, many courts have recognized that mobile app stores are interactive computer services, even though apps are code that communicate information differently than a photo or a video or a social media post. *E.g.*, *Diep v. Apple, Inc.*, 2024 WL 1299995, at *1 (9th Cir. Mar. 27, 2024) (holding that "Apple's App Store" is an interactive computer service); *Coffee v. Google, LLC*,

2022 WL 94986, at *5 (N.D. Cal. Jan. 10, 2022) (concluding that Google's "Play Store" is an interactive computer service).

Understood in light of Section 230's purpose, "information" includes code. One of Congress's purposes in enacting the statute was to preserve the free flow of information over the Internet by shielding intermediaries from liability arising from their hosting of objectionable third-party content. This Court and many others have recognized that given the "'staggering'" amount of information communicated over the Internet, "[i]t would be impossible for service providers to screen … for possible problems," and "[f]aced with potential liability" for information they transmitted, "providers might choose to severely restrict" the free flow of information. *Force*, 934 F.3d at 63 (quoting *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997)); *see also, e.g.*, *Bennett v. Google, LLC*, 882 F.3d 1163, 1166 (D.C. Cir. 2018); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123-24 (9th Cir. 2003). "'Congress … chose to immunize service providers to avoid any such restrictive effect.'" *Force*, 934 F.3d at 63 (quoting *Zeran*, 129 F.3d at 331).

In light of this purpose, it would be a mistake to try to distinguish, as the government proposes, between "information for a human audience" and other information such as computer code. Gov't Br. 25. That artificial limit is highly ambiguous, and not merely because it threatens vital platforms for online apps. After all, as further discussed below, everything published on the Internet is a form of

software, as it involves the operation and exchange of computer code. And the Government gives no reliable way to distinguish some forms of software from others. Indeed, the tunes here were clearly intended, on some level, for a human audience: they were marketed to and downloaded by human beings who wished to make certain modifications to their cars. This Court should not accept the government's invitation to plunge Section 230 jurisprudence into a metaphysical quagmire about what is sufficiently human-directed, all without any basis in the text of the statute.

To the contrary, Congress sought through Section 230 immunity to promote the dissemination and exchange of information over the Internet and to protect intermediaries from liability that would stifle the growth of innovative online services that enable that exchange, and lead to a more restricted and less vibrant information ecosystem. Distinguishing between kinds of information reintroduces the very problem Congress sought to solve by creating legal uncertainty for services that host third-party content. The courts of appeal agree that "the text of Section 230(c)(1) should be construed broadly in favor of immunity" in furtherance of this goal. *Force*, 934 F.3d at 64 (collecting cases).

Persuasive authority further confirms that "information" includes code. Despite the government's assertion that "no court appears to have analyzed whether software is 'information,'" Gov't Br. 25, the Third Circuit has rejected the very same

argument the government makes here. In *Green*, a hacker in an AOL chat room sent a user a "punter"—a "destructive signal" or "computer program created by a hacker whose purpose is to halt and disrupt another computer." 318 F.3d at 469. The user sued AOL and argued that Section 230 did not apply because the punter was not "information." Like the government here, Gov't Br. 25-26, the user reasoned that "'information' is restricted to 'communication or reception of knowledge or intelligence, and not an unseen signal that halts someone's computer,'" 318 F.3d at 471. In rejecting that argument, the court noted that the definition of "information" included "signal[s]," and that the victim's "narrow interpretation" of the statute "would run afoul of the intention of Section 230." *Id.* Rather than create a square circuit split, this Court should reject the Government's argument and hold that the delete tunes at issue here qualify as "information" under Section 230.

The government's attempt to marshal text, purpose, and persuasive authority in support of its position misses the mark.[3] Unable to rely on the ordinary meaning of the term "information" to support its argument, the government instead points to other words in the statute. The government argues that the statutory terms "'publisher or speaker' … "strongly suggest communication among people rather

[3] As an initial matter, while the government faults the district court for its concise treatment of whether "software is information," *see* Gov't Br. 26 n.8, the government never argued to the district court that delete tunes were not information. The government therefore "waived this argument by failing to present it below." *In re Nortel Networks Corp. Secs. Litig.*, 539 F.3d 129, 132 (2d Cir. 2008).

than software programs' instructions to computers.'" Gov't Br. 26-27 (quoting 47 U.S.C. § 230(c)(1)). Not so. The term "publisher" means "one that makes public," or "the reproducer of a work intended for public consumption." *Webster's Third New Int'l Dictionary* 1837; *accord* Black's Law Dictionary (11th ed. 2019) (defining "publish" as "[t]o distribute copies (of a work) to the public"); *see Force*, 934 F.3d at 65 (collecting definitions of "publisher"). Even the government's own authority takes as a given that software is something "publish[ed]" by "publisher[s]." S*ee Commodity Futures Trading Comm'n v. Vartuli*, 228 F.3d 94, 101 (2d Cir. 2000) ("software publisher"); *id.* at 108 ("publishing its software"). Regardless, the terms "publisher" and "speaker" cannot be read out of their full context: "publisher or speaker of *any information*." 47 U.S.C. § 230(c)(1) (emphasis added).

The government next claims that Congress's statutory findings emphasize the importance of promoting "communicating information to people, who benefit from hearing and receiving information" and that these findings justify reading "information" to mean "information for a human audience." Gov't Br. 25 (citing 47 U.S.C. § 230(a)(1), (a)(2), (a)(4), (b)(3)). But the government overlooks that construing "information" consistent with its ordinary meaning furthers the purpose of communicating information to people. If interactive computer services were forced to monitor their services for some kinds of information—such as potentially harmful code—services might respond by filtering or blocking any third-party

information that could constitute or include software code or shuttering some forums for speech entirely. For example, if an operator of an app store faced liability for the functional capabilities of any third-party apps distributed through the app store, the operator might respond by shutting down the app store entirely or dramatically restricting the variety of apps available to only those that the operator can thoroughly and continually examine.

Additionally, though fostering "political" and "education" speech is certainly one of Section 230's purposes, it was not the only purpose. 47 U.S.C. § 230(a). Congress also sought generally "to promote the continued development of the Internet and other interactive computer services and other interactive media" and "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." 47 U.S.C. § 230(b)(1)-(2).

Unable to find any cases supporting its erroneous reading of Section 230, the government instead relies on two non-Section-230 decisions that distinguish between the "functional and expressive elements" of computer software in the context of First Amendment challenges. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 451 (2d Cir. 2001); *Vartuli*, 228 F.3d at 111. These decisions shed no light on the meaning of the specific language Congress chose when enacting Section 230. While Section 230 and the First Amendment offer reinforcing protections, the

statute is not limited to constitutionally protected speech. To the contrary, a key purpose of Section 230 is protecting service providers against claims arising from third-party material that may be illegal or unprotected by the Constitution, such as defamation and obscenity. *E.g.*, *Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 26 (2d Cir. 2015). Even assuming that EZ Lynk's tunes would be outside of First Amendment protection, that does not remove them from Section 230's broader ambit.

In all events, the government's argument fails on its own terms because computer code *is expressive*—as recognized by the very cases the government cites. "Like music and mathematical equations, computer language is just that, language, and it communicates information either to a computer or to those who can read it." *Bernstein v. U.S. Dep't of State*, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996). At the outset, the government's argument ignores this Court's holding in *Corley* that software is protected by the First Amendment, regardless of whether it is abstract or executable. *Corley*, 273 F.3d at 448 ("Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both)"). The fact that software "has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information" to humans. *Id.* at 447. "Instructions such as computer code, which are intended to be executable by a computer, will often

convey information capable of comprehension and assessment by a human being." *Id.* Thus, "computer code, and computer programs constructed from code" can "qualify as speech" and "merit First Amendment protection." *Id.* at 448-49; *accord Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000) (holding that "[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programming," it is protected by the First Amendment). Simply put, *Corley* supports the argument that software is included within the broad and ordinary meaning of "information" in Section 230.

B. Carving out code from Section 230 would chill speech and make the Internet less vibrant.

Beyond being contrary to text, precedent, and purpose, arbitrarily carving out computer code from Section 230 would chill the dissemination of information, including speech, and make the Internet less vibrant. That runs counter to a fundamental goal of Section 230—to foster "forum[s] for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." 47 U.S.C. § 230(a)(3).

The government's theory would potentially open the door to claims against interactive computer services based on any third-party code they transmit. Yet virtually every service on the Internet is involved in transmitting "instructions to an electronic system." Gov't Br. 3. Mobile app stores publish software applications, which include the code necessary for the software to operate. Cloud storage services

host computer files, which contain code. Web hosting services host websites, which are written with code. Websites often include third-party content, whether it be user-uploaded content or third-party ads, that may contain code. Carving code out of Section 230 would force these services to either dedicate significant resources to heavily policing all information they disseminate for potentially harmful code (a likely impossible task) or shut down certain platforms entirely.

The facts of *Green* illustrate that the government's theory would have chilling effects across the entire Internet. In *Green*, a hacker in a chat room sent a user a "punter" program that halted and disrupted the user's computer. 318 F.3d at 469. Under the government's interpretation, Section 230 would provide no defense to the chat room operator because the "punter" program merely conveyed harmful "instructions" to the user's computer and did not communicate "information to humans." Gov't Br. 3. But all kinds of services—not just AOL chat rooms—can be vectors for potentially hazardous computer code. And such code could be contained in any kind of material transmitted online: videos, images, text messages, emails, apps. *See generally* Andreea-Ioana Frățilă, *Analysis of Computer Malware and Common Attacks*, 9 Int'l J. Info. Sec. & Cybercrime 38 (December 2020). On the government's theory, Section 230 would offer no protection to online intermediaries when their platforms were misused by third parties to disseminate such material—a state of affairs that opens the door to the heckler's veto problem Section 230 seeks

to solve, *see, e.g.*, *Jones v. Dirty World Ent. Recordings LLC*, 755 F.3d 398, 407-08 (6th Cir. 2014), and that would oblige services to take a much heavier hand in restricting the information users can transmit. Congress would not have intended such a result.

Mobile app stores also illustrate the immense scale of the problems with the government's position. Leading app stores offer users around the world nearly two million apps each. *See* Apple, *App Store*, https://www.apple.com/app-store/; Google, *How Google Play Works*, https://play.google.com/about/howplayworks/. An app might contain hundreds of thousands or millions of lines of code. In the government's view, Section 230 provides no defense to the operators of app stores for claims based on the function of the apps. As it stands now, app stores go to great lengths to protect their users from malware. *See, e.g.*, Apple, *About App Store Security*, https://support.apple.com/guide/security/about-app-store-security-secb8f887a15/web; Google Play, *Google Play Protect*, https://developers.google.com/android/play-protect. But without Section 230's protections, platforms would be forced to (1) inspect the code of each app, (2) shrink or shut down their app stores, or (3) risk a lawsuit and ruinous liability each time a user believes an app contained malicious code that harmed him.

The government's position, if adopted, would create the same dilemma for virtually every Internet service because code is omnipresent—it is "the brick and

mortar of cyberspace." Jorge R. Roig, *Decoding First Amendment Coverage of Computer Source Code in the Age of YouTube, Facebook, and the Arab Spring*, 68 N.Y.U. Ann. Surv. Am. L. 319, 396 (2012). Services, users, and the broader Internet ecosystem will be harmed if providers of app stores and other digital distribution services are essentially forced by the threat of vexatious litigation to meticulously review all third-party code before distribution. The result would be fewer options, less speech, and a less safe Internet.

II. The Government's Claim Treats Defendants As The Publisher Or Speaker Of The Delete Tunes.

The government's theory of liability treats Defendants as "publishers" because it seeks to hold Defendants liable for providing a forum for third parties to disseminate delete tunes. But that alleged conduct "falls within the heartland of what it means to be the 'publisher' of information under Section 230(c)(1)." *Force*, 934 F.3d at 65 (allegation that Facebook gave "Hamas a forum with which to communicate" and "actively br[ought] Hamas' message to interested parties" fell within the "heartland" of publishing). Defendants operate the "EZ Lynk Cloud[, which] enables drivers to acquire delete tunes." JA-26 ¶ 51. And the government's claim seeks to hold Defendants liable for traditional editorial functions, *i.e.*, their decisions about "'whether to publish, withdraw, postpone or alter'" the third-party delete tunes available on the EZ Lynk Cloud. *Force*, 934 F.3d at 81 (quoting *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 174 (2d Cir. 2016)).

The government's "duty to monitor" theory confirms that its Clean Air Act claim seeks to hold Defendants liable as publishers of third-party information. One way a claim can treat the defendant as a publisher is where the duty at issue "obliges the defendant to 'monitor third-party content'—or else face liability." *Calise v. Meta Platforms, Inc.*, 103 F.4th 732, 742 (9th Cir. 2024) (quoting *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 682 (9th Cir. 2019)). The claim here makes it illegal for a person "to manufacture or sell" a "part or component intended for use with … any motor vehicle" if "a principal effect" of the part or component is to "defeat" emissions controls "and where the person knows or should know" that it is "put to such use." 42 U.S.C. § 7522(a)(3)(B). The government alleges that the EZ Lynk System has the requisite principal effect of defeating emissions controls because of delete tunes created by third parties. *See* JA-40 ¶ 94. The only way for EZ Lynk to comply with its duty here would be to monitor the tunes available on the EZ Lynk Cloud and remove delete tunes. Accordingly, the claim treats Defendants as the publisher of the delete tunes, and Section 230 bars the claim.

The government makes much of the fact that the EZ Lynk System includes a "hardware" component, Gov't Br. 2, 22, 24, 31, but that is a red herring. As the government admits, its claim is based on the EZ Lynk System as a "whole." Gov't Br. 33. Moreover, as the district court ruled—and as the government does not dispute, Gov't Br. 17 n.3—the EZ Lynk System's hardware component does not by

itself trigger liability. JA-118 ("The Auto Agent, by itself, cannot have 'a principal effect' of defeating emissions controls, and Section 203 of the Clean Air Act does not prohibit selling merely one part of a prohibited 'part.'"). The third-party delete tunes are essential to the government's claim; without them, the EZ Lynk System would not have the "principal effect" of "bypass[ing], defeat[ing], or render[ing] intraoperative" an Emission Related Element of Design. *Cf.* JA-40 ¶ 94 ("Many of *the tunes used with the EZ Lynk System* bypass, defeat, or render inoperative the [vehicle's] software[, which] is an Emission Related Element of Design." (emphasis added)).

Any holding that a defendant loses Section 230 protection simply by bundling hardware with software would strike at the roots of the Internet ecosystem. All kinds of devices, from phones to tablets to televisions to computers and virtually all devices that people use to access the Internet, are made with "smart" capabilities that enable access to third-party software. These devices and the third-party software accessed through them have immense public benefits, as anyone with a smartphone can attest. But the same theory the government advances here could upend that information ecosystem by exposing smart-device makers to liability on the theory that they provide "the tools necessary … to access the software." Gov't Br. 33. The Court should make clear that just because a claim involves a defendant's hardware does not mean they lose Section 230's protection.

III. Section 230 Should Be Applied At The Earliest Possible Opportunity, Including As A Ground For Dismissal.

The government argues that the district court was "particularly" "wrong" to dismiss the complaint based on an affirmative defense, Section 230. Gov't Br. 3. But there is nothing wrong or even unusual in dismissing a claim barred by Section 230 at the pleading stage. As the government admits, affirmative defenses, including Section 230, can be a basis for dismissal at the 12(b)(6) stage, so long as "'the statute's barrier to suit is evident from the face of the complaint.'" Gov't Br. 25 (quoting *Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 28 (2d Cir. 2015)). And in fact, binding circuit precedent supports the district court's application of Section 230 at the motion-to-dismiss stage.

A. The district court correctly applied Section 230 at the motion-to-dismiss stage.

Dismissals based on Section 230 are routine and were intended to be so. This Court has expressly held that "the application of Section 230(c)(1) is appropriate at the pleading stage." *Force*, 934 F.3d at 63 n.15; *accord Ricci*, 781 F.3d at 28 (holding that Section 230 can "support a motion to dismiss"). And it has itself affirmed Section 230 dismissals at least three times. *E.g.*, *Force*, 934 F.3d at 57; *Ricci*, 781 F.3d at 28; *Herrick v. Grindr LLC*, 765 F. App'x 586, 589 (2d Cir. 2019). Section 230 dismissals are routine for good reason.

Congress intended Section 230 to provide immunity from suit as well as a defense to liability: "[n]o cause of action may be brought and no liability may be imposed." *See* 47 U.S.C. § 230(e)(3). Accordingly, courts have recognized that Section 230 "is an immunity from suit rather than a mere defense to liability," *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009), and it "protect[s] websites not merely from ultimate liability, but [also] from having to fight costly and protracted legal battles." *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1175 (9th Cir. 2008) (en banc). As such, courts should and do apply it "at the earliest possible stage of the case." *Nemet*, 591 F.3d at 255.

In particular, the government objects that it had no obligation "to plead that EZ Lynk itself acted as an information content provider." Gov't Br. 37. But given the express allegation that delete tunes were provided by "[t]hird-party companies and individuals," JA-26 ¶ 50; *see also* Gov't Br. 2, the district court was correct to then require the government to plausibly allege that Defendants were "responsible" for the "creation or development" of the third-party delete tunes. *See* 47 U.S.C. § 230(f)(3).

Courts recognize that where a complaint alleges that the offending content is provided by a third party, Section 230 immunity applies unless the complaint plausibly alleges that "the defendant directly and 'materially' contributed to what

made the [third-party] content itself 'unlawful.'" *Force*, 934 F.3d at 68 (quoting *Leadclick*, 838 F.3d at 174). This Court did exactly that in *Force*. *See* 934 F.3d at 68-69 (assessing "whether Facebook is plausibly alleged to *itself* be an 'information content provider,' or whether it is Hamas that provides all of the complained-of content"). And so have other courts. *See, e.g.*, *Rigsby v. GoDaddy Inc.*, 59 F.4th 998, 1008-09 (9th Cir. 2023); *E. Coast Test Prep LLC v. Allnurses.com, Inc.*, 971 F.3d 747, 752 (8th Cir. 2020); *Small Just. LLC v. Xcentric Ventures LLC*, 873 F.3d 313, 322 (1st Cir. 2017). Any other approach would render Section 230 "meaningless as a practical matter," because "[w]ebsites are complicated enterprises, and there will always be close cases where a clever lawyer could argue that *something* the website operator did encouraged the illegality." *Roommates.com*, 521 F.3d at 1174 (en banc).

B. Early adjudication of Section 230 defenses furthers Congress's goals of fostering the development of the Internet and minimizing chilling effects on speech.

Courts can often determine whether Section 230(c)(1) bars a claim based solely on the facts alleged in the complaint, and those cases can be quickly and cost-effectively resolved on motions to dismiss. This early and efficient adjudication of Section 230 defenses furthers Congress's policy goals in enacting Section 230 to the immense benefit of both interactive computer services and their users. *See* Eric

Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 Notre Dame L. Rev. Reflection 33, 41-42 (2019).

Screening out cases clearly barred by Section 230 at the motion-to-dismiss stage benefits users and the public by blunting the power of a "'heckler's veto' that would chill free speech." *Jones*, 755 F.3d at 407. A troubling number of Section 230 cases involve plaintiffs who sought to use the threat of litigation as a heckler's veto. *See* Elizabeth Banker, *Understanding Section 230 & the Impact of Litigation on Small Providers* 30-50, Chamber of Progress (2022) (collecting cases). Faced with the prospect of expensive litigation over someone else's information, the rational choice for a business will be to remove content rather than pay to defend it. To their credit, a remarkable number of digital services stood firm against legal threats and lawsuits to defend their right to keep the speech of others online. Without Section 230, it would be far harder, and significantly more expensive, for websites to stand their ground. The opportunity for early termination of lawsuits helps shift the calculus in favor of more speech and greater diversity by sparing platforms from the costs of discovery, summary judgment and trial.

Early adjudication of Section 230 defenses is especially vital for small business, startup companies, and their users. The cost of defending even one frivolous claim can easily exceed a startup's valuation. *See* Evan Engstrom, *Primer: Value of Section 230*, Engine (Jan. 31, 2019),

https://www.engine.is/news/primer/section230costs. The risk of business-ending litigation impacts the ability of startups to attract funding and the cost-benefit analysis for entities who want to offer an interactive forum but know it will not produce significant revenue. *See* Banker, *supra*, at 7. Thus, "[t]he ability of a defendant to resolve a case on a motion to dismiss (and avoiding expensive discovery) protects small and low-revenue Internet services, which in turn enhances the richness and diversity of the Internet ecosystem." Goldman, *Why Section 230 Is Better Than the First Amendment*, *supra*, at 41; *see also* 47 U.S.C. § 230(b)(1)-(2) (stating the policy of the United States to "promote the continued development" of Internet services and to "preserve the vibrant and competitive free market").

CONCLUSION

When it enacted Section 230, Congress sought to shield websites from liability so that the public could benefit from the development of the Internet and the free flow of information. The government's arguments—about the meaning of "information," whether its claim treats Defendants as the publisher of delete tunes, and how the district court applied Section 230 at the motion-to-dismiss stage—run contrary to the text and purpose of Section 230 and, if adopted, would harm the Internet ecosystem and all who benefit from it.

Dated December 20, 2024

Respectfully submitted,

/s/ Paul N. Harold

Brian M. Willen
Wilson Sonsini Goodrich & Rosati, P.C.
1301 Ave. of the Americas, 40th Floor
New York, NY 10019
(212) 999-5800
bwillen@wsgr.com

Lauren Gallo White
Wilson Sonsini Goodrich & Rosati, P.C.
One Market Plaza, Spear Tower, Ste 3300
San Francisco, CA 94105
(415) 947-2000
lwhite@wsgr.com

Paul N. Harold
Steffen N. Johnson
Wilson Sonsini Goodrich & Rosati, P.C.
1700 K Street, N.W.
Washington, D.C. 20004
(202) 973-8800
pharold@wsgr.com
sjohnson@wsgr.com

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Federal Rule of Appellate Procedure 32(g), the undersigned counsel hereby certifies that this brief complies with the type-volume limitation of the Federal Rules of Appellate Procedure and this Court's Local Rules. As measured by the word processing system used to prepare this brief, there are 6,420 words in this brief.

Dated: December 20, 2024

/s/ Paul N. Harold
Paul N. Harold