Nos. 22-16914 & 22-16916

IN THE

# United States Court of Appeals for the Ninth Circuit

IN RE: APPLE INC. APP STORE
SIMULATED CASINO-STYLE GAMES LITIGATION

FRANK CUSTODERO, et al.,

*Plaintiffs-Appellees,*

v.

APPLE, INC.,

*Defendant-Appellant.*

On Cross-Appeals from the United States District Court
for the Northern District of California
No. 5:21-md-02985-EJD (Hon. Edward J. Davila)

**BRIEF OF AMICI CURIAE CHAMBER OF PROGRESS AND NETCHOICE IN SUPPORT OF DEFENDANT-APPELLANT APPLE INC.**


Mark W. Brennan
Sean Marotta
J. Ryan Thompson
Andrew McCardle
HOGAN LOVELLS US LLP
555 13th Street NW
Washington, DC 20004
Telephone: (202) 637-5600

*Counsel for Amici Curiae*
*Chamber of Progress and NetChoice*

Jess Miers
Legal Advocacy Counsel
CHAMBER OF PROGRESS
1390 Chain Bridge Road #A108
McLean, VA 22101

Nicole Saad Bembridge
Associate Counsel
NETCHOICE
1401 K Street NW, Suite 502
Washington, DC 20005

## CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, the undersigned counsel of record states that, as nonprofit entities organized under § 501(c)(6) of the Internal Revenue Code, amici curiae Chamber of Progress and NetChoice L.L.C. have issued no stock. Consequently, no parent corporation nor any publicly held corporation could or does own 10% or more of their stock.

*s/ Sean Marotta*
Sean Marotta

*Counsel for Amici Curiae*
*Chamber of Progress and NetChoice*

## TABLE OF CONTENTS

**Page**


CORPORATE DISCLOSURE STATEMENT ..... i

TABLE OF AUTHORITIES ..... iv

STATEMENT PURSUANT TO FED. R. APP. P. 29(a)(4)(E) ..... 1

AMICI'S IDENTITIES, INTERESTS, AND AUTHORITY TO FILE THIS BRIEF ..... 1

INTRODUCTION ..... 3

ARGUMENT ..... 5

I. SECTION 230 SHIELDS ONLINE PUBLISHERS FROM PAYMENT-RELATED CLAIMS ARISING FROM THIRD-PARTY SPEECH, ENABLING THE SERVICES TO SUPPORT THE CREATOR ECONOMY AND PROTECT CONSUMERS ..... 5

A. Section 230 Bars Payment-Based Theories of Liability That Would Create a Duty to Monitor and to Modify or Remove Third-Party Content ..... 6

B. Plaintiffs' Payment Processor Theory of Liability Would Discourage the Services and Online Marketplaces from Supporting In-App Payments ..... 9

C. Plaintiffs' Theory of Liability Also Presents Serious Consumer Safety and Security Risks ..... 12

II. AFFIRMING SECTION 230'S ESSENTIAL PROTECTIONS FOR ALGORITHMIC CURATION WILL BENEFIT INTERNET USERS AND APP DEVELOPERS, ESPECIALLY MARGINALIZED SPEAKERS AND AUDIENCES EXPRESSING DISSENT ..... 16

A. Section 230's Protections for Content Curation Are Essential to the Basic Functioning of App Stores ..... 17

B. Withdrawing Section 230's Protections for Content Curation Would Especially Harm Marginalized Speakers and Audiences ..... 18

## TABLE OF CONTENTS—Continued

**Page**

CONCLUSION.....22

CERTIFICATE OF COMPLIANCE

CERTIFICATE OF SERVICE

## TABLE OF AUTHORITIES

**Page**

**CASES:**

*Almeida v. Amazon.com, Inc.*,
456 F.3d 1316 (11th Cir. 2006) .....6

*Barnes v. Yahoo!, Inc.*,
570 F.3d 1096 (9th Cir. 2009) .....5, 7

*Batzel v. Smith*,
333 F.3d 1018 (9th Cir. 2003) .....4

*Doe v. Internet Brands, Inc.*,
824 F.3d 846 (9th Cir. 2016) .....3, 7

*Epic Games, Inc. v. Apple Inc.*,
559 F. Supp. 3d 898 (N.D. Cal. 2021) ..... 14, 15

*Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*,
521 F.3d 1157 (9th Cir. 2008) .....6, 9

*Gonzalez v. Google LLC*,
2 F.4th 871 (9th Cir. 2021) .....8

*HomeAway.com, Inc. v. City of Santa Monica*,
918 F.3d 676 (9th Cir. 2019) .....7, 8

*Jane Doe No. 1 v. Backpage.com, LLC*,
817 F.3d 12 (1st Cir. 2016).....6

*Jones v. Dirty World Entm't Recordings LLC*,
755 F.3d 398 (6th Cir. 2014) .....6

*Kimzey v. Yelp! Inc.*,
836 F.3d 1263 (9th Cir. 2016) .....3

*Perfect 10, Inc. v. CCBill LLC*,
488 F.3d 1102 (9th Cir. 2007) .....6

*Zeran v. America Online, Inc.*,
129 F.3d 327 (4th Cir. 1997) .....6

## TABLE OF AUTHORITIES—Continued

**Page**

**STATUTES:**

47 U.S.C. § 230 ..... *passim*

47 U.S.C. § 230(b)(2) ..... 4

47 U.S.C. § 230(c)(1) ..... 5, 17

**OTHER AUTHORITIES:**

*2022 App Store Transparency Report*, Apple (2023) ..... 17

Kendra Albert et al., *FOSTA in Legal Context*, 52 COLUM. HUM. RTS. L. REV. 1084 (2021) ..... 19

Stacy Cowley & Lananh Nguyen, *Fraud is Flourishing on Zelle. The Banks Say it's not their Problem*, N.Y. TIMES (Mar. 6, 2022) ..... 13, 14

DEP'T OF THE TREASURY, NATIONAL MONEY LAUNDERING RISK ASSESSMENT (2022) ..... 14

*Digital Literacy for Senior Citizens: Building ICT Competencies*, Institute of Electrical and Electronics Engineers (Jul. 18, 2023) ..... 16

Tarleton Gillespie, *Do Not Recommend? Reduction as a Form of Content Moderation*, SOC. MEDIA + SOC'Y (July-Sept. 2022) ..... 18

Eric Goldman, *Content Moderation Remedies*, 28 MICH. TECH. L. REV. 1 (2021) ..... 17, 18

Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 NOTRE DAME L. REV. 33 (2020) ..... 17

Eric Goldman & Jess Miers, *Online Account Terminations/Content Removals and the Benefits of Internet Services Enforcing Their House Rules*, 1 J. FREE SPEECH L. 191 (2021) ..... 20

*How Google Play works*, Google ..... 17

Jennifer Huddleston, *Competition and Content Moderation: How Section 230 Enables Increased Tech Marketplace Entry*, Cato Inst. (2022) ..... 20

## TABLE OF AUTHORITIES—Continued

**Page**


Mansoor Iqbal, *App Revenue Data (2023)*, BUSINESS OF APPS (May 2, 2023) .....10

JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019) .....17

Letter from Chamber of Progress to Merrick B. Garland, U.S. Att'y Gen. (Nov. 21, 2022) .....19

*Managing Risks in Third-Party Payment Processor Relationships*, FDIC (June 23, 2023) .....14

Jack Nassetta & Kimberly Gross, *State Media Warning Labels Can Counteract the Effects of Foreign Misinformation*, HARV. KENNEDY SCH. MISINFORMATION REV. (Oct. 30, 2020) .....20

Office of Servicemember Affairs Annual Report, CFPB (June 20, 2023) .....13

Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, Pew Research Center (Jan. 26, 2017) ..... 15, 16

*Payment Orchestration Helps Conversion Rates – And Merchants' Margins*, PYMNTS (Aug. 25, 2021) .....11

Nathaniel Popper, *When Your Last $166 Vanishes: 'Fast Fraud' Surges on Payment Apps*, N.Y. TIMES (Oct. 11, 2020) .....13

Press Release, Apple, *App Store developers generated $1.1 trillion in total billings and sales in the App Store ecosystem in 2022* (May 31, 2023) .....11

Press Release, CFPB, *Consumer Financial Protection Bureau takes Action Against Payment Processor and Its Former CEO for Supporting Internet-Based technical-Support Scams* (Mar. 3, 2021) .....14

Shuo-Chang Tsai et al., *Exploring Transaction Security on Consumers' Willingness to Use Mobile Payment by Using the Technology Acceptance Model*, 5 APPLIED SYSTEM INNOVATION 113 (2022) .....11

Emily A. Vogels and Monica Anderson, *Americans and Digital Knowledge*, Pew Research Center (Oct. 9, 2019) .....16

## STATEMENT PURSUANT TO FED. R. APP. P. 29(a)(4)(E)

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; and no person other than the amici curiae, their members, or their counsel contributed money that was intended to fund preparing or submitting this brief.

## AMICI'S IDENTITIES, INTERESTS, AND AUTHORITY TO FILE THIS BRIEF

**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. In keeping with that mission, Chamber of Progress believes that allowing a diverse range of app-store models and philosophies to flourish will benefit everyone—consumers, store owners, and application developers.

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.[1]

**NetChoice** is a national trade association of online businesses that share the goal of promoting free enterprise and free expression on the Internet. NetChoice's members operate a variety of popular websites, apps, and online services, including Meta (formerly Facebook), YouTube, and Etsy.[2] NetChoice's guiding principles are (1) promoting consumer choice, (2) continuing the successful policy of "light-touch" Internet regulation, and (3) fostering online competition to provide consumers with an abundance of services.

Both amici are concerned about the disruption to the app markets that could result from this litigation, ultimately harming consumers and the creator economy that Apple, Google, and Meta ("Services") support. In particular, amici worry that, if the Court affirms the district court's rationale that app store operators who provide payment services can be held liable for apps that use those payment services, app store operators will be forced to monitor all activity on their app store or remove payment processing services for many or all apps.

All parties have granted Chamber of Progress and NetChoice permission to

---

[1] Chamber of Progress's partners include Airbnb, Amazon, Apple, Automattic, Chime, Circle, CLEAR, Coinbase, Creative Juice, Cruise, DoorDash, Earnin, Google, Grayscale, Grubhub, Heirloom Carbon, Instacart, itselectric, Lyft, Meta, Paradigm, Pindrop, Ripple, SmileDirectClub, StubHub, Turo, Uber, Waymo, Zillow, and Zoox.

[2] A list of NetChoice's members is available at https://netchoice.org/about.

file this amicus brief. *See* Fed. R. App. P. 29(a); Circuit Advisory Committee Note to Rule 29-3.

## INTRODUCTION

Litigants cannot circumvent Section 230's protections through "creative pleading." *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1265 (9th Cir. 2016). Plaintiffs have attempted to recast the Services from publishers to payment processors. But the Services' neutral payment processing activities—which Plaintiffs do not allege are inherently unlawful—are inextricable from the third-party-generated casino apps underlying all of Plaintiffs' claims. Plaintiffs' theory of liability would require the Services to monitor all third-party content, which several courts have held is subject to Section 230. *See, e.g.*, *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 852-54 (9th Cir. 2016).

That is not the only way in which Section 230 protects the Services against Plaintiffs' claims. Plaintiffs' theory would also effectively require the Services to (1) remove from their app stores any third-party app that uses the Services' neutral payment processing services if the Platform suspects there is any violative third-party content in the app or (2) require the app developer to eliminate the violative content. Exercising editorial discretion, which includes decisions to remove and modify content, are not only fundamental examples of publisher rights granted by the First Amendment but also activities fully protected under Section 230. *Id.* But

faced with these alternatives, the Services may very well forgo offering payment services for some or all apps altogether.

Permitting a payment-processor loophole in Section 230 would thwart Congress's goal of promoting a vibrant, innovative Internet and e-commerce ecosystem. *See Batzel v. Smith*, 333 F.3d 1018, 1027 (9th Cir. 2003); 47 U.S.C. § 230(b)(2) ("It is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet . . . ."). If the Court adopts Plaintiffs' theory of Section 230 liability, app developers could be deprived of key functionality and safe transaction tools that are integral to the Services' trusted app marketplaces. *Id.* For small app developers with limited or no resources to invest in facilitating payment processing, this could be particularly harmful.

Consumers and other online users, app developers, and the broader Internet ecosystem will also be harmed if the Services are essentially forced by the threat of vexatious litigation to remove their neutral payment processing services from app stores and online marketplaces. For example, rather than being able to rely on the trusted payment tools and other e-commerce safeguards that the Services have made available, users will be put in the impossible position of vetting every app developer with which they would like to transact. And malicious actors would almost certainly seize the opportunity to engage in identity theft, scams, and other fraudulent activity.

Finally, the Court should also affirm the district court's determination that

Section 230 protects algorithmic curation of an app store, including for listing the casino apps. Algorithmic curation is a core editorial function protected by Section 230. It empowers online platforms to help users find the content they want and to express each platform's own preferences regarding the content hosted. Moreover, limiting or eliminating Section 230's protections is likely to harm marginalized voices that rely on the Services' app stores to distribute their apps.

The Court should reverse the district court's holding that Section 230 does not shield publishers that also offer payment services. It should also affirm the district court's determination that Section 230 protects the Services from claims that they are liable for listing the casino apps.

## ARGUMENT

### I. SECTION 230 SHIELDS ONLINE PUBLISHERS FROM PAYMENT-RELATED CLAIMS ARISING FROM THIRD-PARTY SPEECH, ENABLING THE SERVICES TO SUPPORT THE CREATOR ECONOMY AND PROTECT CONSUMERS.

Section 230(c)(1) protects online app store operators from liability based on information provided by third parties when (1) a party is a "provider or user of an interactive computer service," and (2) a law treats the party "as a publisher or speaker" (3) "of information provided by another information content provider." *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100-01 (9th Cir. 2009). The first and third factors are met. ER-33. The only disagreement is over whether the Services are

being treated as "publishers" for purposes of Section 230.

But this Court has emphasized Section 230's "broad grant" of protection for "webhosts," like the Services, as publishers or speakers. *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1174-75, 1180 (9th Cir. 2008) (en banc). Other circuits have held likewise. *See, e.g.*, *Jones v. Dirty World Entm't Recordings LLC*, 755 F.3d 398, 407 (6th Cir. 2014). Section 230 "establish[es] broad 'federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.'" *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118 (9th Cir. 2007) (quoting *Almeida v. Amazon.com, Inc.*, 456 F.3d 1316, 1321 (11th Cir. 2006) and *Zeran v. America Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997)); *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 19 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017). Given Section 230's breadth, "close cases . . . must be resolved in favor of immunity." *Roommates.com*, 521 F.3d at 1174.

### A. Section 230 Bars Payment-Based Theories of Liability That Would Create a Duty to Monitor and to Modify or Remove Third-Party Content.

Plaintiffs' theory of liability treats the Services as "publishers" of third-party information by requiring them to monitor and to modify or remove content of third-party apps. Plaintiffs concede as much, arguing that the Services "did not remove social casinos from their offerings," ER-159, and did not take "steps to limit access

to" the casino apps. ER-160.

Obligations to monitor and review third-party content are paradigmatic activities that Section 230 preempts. The Court has repeatedly held that "publication involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content." *Barnes*, 570 F.3d at 1102.

*Internet Brands* illustrates the line between legal obligations that do and do not conflict with Section 230. In that case, the Court drew a sharp line between causes of action that require website operators to monitor third-party website content (from which websites are immune under Section 230) and those that do not require monitoring. *Internet Brands* turned on the fact that the alleged duty to warn under California law would not "affect" how the website "monitors . . . content." 824 F.3d at 851. The Court stressed that the website's "failure to monitor postings" was not "at issue," and it held that "Doe's failure to warn claim has nothing to do with Internet Brands' efforts, or lack thereof, to edit, *monitor*, or *remove* user generated content." *Id.* at 852 (emphasis added). Put differently, the question under *Internet Brands* is whether "the underlying duty 'could have been satisfied without changes to content posted by the website's users.'" *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 683 (9th Cir. 2019) (quoting *Internet Brands*, 824 F.3d at 851).

The district court reasoned that this case is like *Internet Brands*, *HomeAway*,

and *Gonzalez v. Google LLC*, 2 F.4th 871 (9th Cir. 2021) because Plaintiff's theory of liability involves transactions that the Services allegedly facilitated. But this overlooks a key part of the analytical framework: Section 230 bars claims that would create a "duty [that] would necessarily require an [I]nternet company to monitor third-party content." *HomeAway*, 918 F.3d at 682.

Here, it is the casino apps' functionality as a "virtual casino" for which the Services are allegedly liable for facilitating transactions. The allegedly unlawful transactions are inextricable from the casino apps themselves (i.e., third-party content).

Under Plaintiffs' theory of liability, the Services would need to do the following to avoid liability (1) monitor all apps that support in-app payments and (2) remove the seemingly unlawful casino app from their app stores or require the app developers to modify the app to remove the Services' payment processing tool. Those duties would conflict with Section 230 and be preempted.

How else could the Services uphold a legal duty to not provide payment processing services to violative applications other than to monitor each app's functionality? Services could not rely on the purported descriptions provided by the app developers because the descriptions could be inaccurate and the apps (and their functionality) constantly evolve. The Services would need to test every app—including after every app update—to determine whether and how much each

payment opportunity provided in the app constituted a seemingly unlawful transaction. What's more, they would also likely err on the side of removal of the app or disabling payment services rather than risk liability.

There is also nothing inherently unlawful with the neutral payment processing services the Services offer. The Services offer all app developers the same set of content-neutral tools. *Roommates.com, LLC*, 521 F.3d at 1169 ("[P]roviding neutral tools to carry out what may be unlawful or illicit searches does not amount to 'development' for purposes of the immunity exception."). If third-party app developers create virtual content that they wish to offer for sale to consumers through their apps, the Services offer payment processing services for those transactions. Nowhere do Plaintiffs identify how the payment processing offered for the gaming apps differs from the payment processing service provided to all developers regardless of any particular app's content.

For these reasons, the Court should view Plaintiff's theory of payment processor liability for what it is: publisher liability in all but name, and thus also reverse the district court's denial of the Services' motions to dismiss based on Plaintiffs' flawed theory.

### B. Plaintiffs' Payment Processor Theory of Liability Would Discourage the Services and Online Marketplaces from Supporting In-App Payments.

If the Court were to adopt Plaintiffs' theory that the Services are liable for

third-party content when they also offer neutral payment services, Services would be forced to either: (1) dedicate significant resources heavily policing millions of apps (and app updates) that use the Services' payment processing services or (2) remove payment processing services altogether. The first option may not even be feasible, given the number of apps available on each platform, and the frequency of each app update. The second option opens a dangerous Pandora's box of safety issues for consumers who will endure the heightened risk of fraud, phishing, identity theft, and abuse as they try to navigate what was once a safe and predictable process.

The Services' payment processing services provide crucial support for app developers, as well as the broader creator economy and Internet ecosystem. In 2022 alone, the Services' payment services supported tens of billions of dollars in in-app purchases. Mansoor Iqbal, *App Revenue Data (2023)*, BUSINESS OF APPS (May 2, 2023), https://bit.ly/44KuVWp. And by offering seamless payment experiences, robust security measures, global accessibility, and valuable insights, these payment platforms empower developers to focus on their creative endeavors and contribute to the flourishing digital marketplace.

***Streamlined In-App Purchases***. By integrating these payment systems, app developers can offer a seamless and secure payment experience within their applications. This frictionless payment flow increases user convenience, leading to higher conversion rates and improved monetization for developers. *See, e.g.*,

*Payment Orchestration Helps Conversion Rates – And Merchants' Margins*, PYMNTS (Aug. 25, 2021), https://bit.ly/43PvM6N.

***Enhanced Security and Trust.*** The Services prioritize user security in payment processing, using tools like tokenization and biometric authentication to safeguard sensitive payment information. For app developers, this commitment to security fosters trust among users, encouraging them to make purchases with confidence. The assurance of safe transactions helps build a loyal customer base and drive revenue growth. Shuo-Chang Tsai et al., *Exploring Transaction Security on Consumers' Willingness to Use Mobile Payment by Using the Technology Acceptance Model*, 5 APPLIED SYSTEM INNOVATION 113 (2022).

***Global Reach and Accessibility.*** These payment tools have a wide international presence, providing app developers with access to a vast global audience. By accepting payments from users in multiple countries and currencies, the Services enable developers to expand their market reach and tap into a diverse consumer base. *See, e.g.*, Press Release, Apple, *App Store developers generated $1.1 trillion in total billings and sales in the App Store ecosystem in 2022* (May 31, 2023), https://apple.co/43LCtH8 ("The App Store's engine of commerce provides Apple developers around the world with a global distribution platform that supports more than 195 local payment methods and 44 currencies across 175 storefronts.").

***Support for Subscription Models.*** The creator economy heavily relies on

subscription-based revenue models. Appellee Supplemental Excerpts of Record, *Epic Games, Inc. v. Apple Inc.*, Docket Nos. 21-16506 & 21-16695, at SER43 (filed Mar. 24, 2022) ("The overwhelming majority of in-app revenue for nongame apps, on the other hand, is from subscription in-app purchases."). Support for recurring payments makes it convenient for developers to offer subscription services to their users. This recurring revenue stream provides developers with a stable income and encourages ongoing content creation.

In sum, the creator economy the Services support with their app stores will suffer if the Court affirms Plaintiffs' theory of payment processor liability.

### C. Plaintiffs' Theory of Liability Also Presents Serious Consumer Safety and Security Risks.

If the Services decline to offer in-app payment tools, developers will have to find alternative payment processing tools, raising a slew of safety and security concerns for users. Currently, consumers know what to expect when they engage with the Services' payment processing tools. They know and expect that their financial information will be kept secure by the payment processors supporting the Services, and the Services can often promptly identify when a user may be subject to phishing, smishing, scams, and other fraudulent tactics. Steering consumers to external payment mechanisms would disrupt this status quo, eradicating consumers' fluency with existing services and exposing them far more often to the risks created when external payment links are used. This result would severely undermine user

confidence in the safety, security, and reliability of digital content purchases and mechanisms.

***Substantial Consumer Risks.*** These risks are not merely hypothetical. An influx of users to payment app services in recent years has come with a corresponding surge in fraud and scams. Nathaniel Popper, *When Your Last $166 Vanishes: 'Fast Fraud' Surges on Payment Apps*, N.Y. TIMES (Oct. 11, 2020), https://nyti.ms/3q86QcP. Between 2018 and 2021, complaints to the Federal Trade Commission ("FTC") about fraud on payment apps increased 460%, totaling more than 70,000 complaints comprising more than $130 million dollars in estimated financial losses. Office of Servicemember Affairs Annual Report, CFPB (June 20, 2023), https://bit.ly/3DAvKFe. One mother of three lost $560, roughly a month's worth of child support, after receiving what appeared to be legitimate requests on Cash App. *Id.* Another user lost a similar sum after interacting with whom he believed to be an official who turned out to be a scammer. Stacy Cowley & Lananh Nguyen, *Fraud is Flourishing on Zelle. The Banks Say it's not their Problem*, N.Y. TIMES (Mar. 6, 2022), https://nyti.ms/44MZsCH. And other users, including many service members who frequently must relocate and thus rely on digital payment apps, have lost thousands of dollars. Office of Servicemember Affairs Annual Report, CFPB (June 20, 2023) ("According to a recent AARP study, servicemembers are nearly 40% more likely to lose money to scams and fraud than

the civilian population.").

Regulators are increasingly warning consumers against the dangers associated with third-party payment processors. In recent years, both the Consumer Finance Protection Bureau and the FTC have pursued enforcement actions against payment processing companies that facilitate credit card laundering, exploit small businesses, support scammers, and defraud consumers. *See, e.g.*, Press Release, CFPB, *Consumer Financial Protection Bureau takes Action Against Payment Processor and Its Former CEO for Supporting Internet-Based technical-Support Scams* (Mar. 3, 2021), https://bit.ly/458uMLV. The Federal Deposit Insurance Commission and Department of the Treasury have likewise warned financial institutions against potentially abusive, fraudulent, high-risk, and illegal practices by third-party payment processors. *Managing Risks in Third-Party Payment Processor Relationships*, FDIC (June 23, 2023), https://bit.ly/3rHJACS; DEP'T OF THE TREASURY, NATIONAL MONEY LAUNDERING RISK ASSESSMENT (2022). Despite these warnings from regulators, consumers remain left to fend for themselves. Cowley & Nguyen.

***Benefits of In-App Purchase Restrictions.*** To combat these risks, platforms like Apple and Google require all in-app purchases on their devices to use the company's own payment processor. *See, e.g.*, *Epic Games, Inc. v. Apple Inc.*, 559 F. Supp. 3d 898, 1002 (N.D. Cal. 2021); *see also* Joint Brief of Chamber of Progress

and NetChoice, Docket Nos. 21-16506 and 21-16695, at 17-21 (filed June 20, 2023) ("Joint Brief") (describing the security risks created by off-app services and content). These in-app purchasing restrictions provide benefits to consumers. For example, platforms can offer users a curated ecosystem. Joint Brief at 20. Restricting external payment processing enables platforms to enhance privacy, quality, and trustworthiness while also thwarting social-engineering attacks that evade a mobile device's operating-system defenses by tricking users into granting access. *Epic Games, Inc.* at 1003-05. Or as Apple's Senior Director of App Review put it, "[w]hen users utilize external payment links, they are thus no longer utilizing a payment mechanism that Apple secures, verifies, and protects from fraud." Joint Brief at 20 (internal quotation omitted). Effectively requiring platforms known for their security to host links to external payment processors is like requiring an auto manufacturer that touts the safety of its cars to post advertisements inside its cars for other cars that are less safe.

***Digital Literacy.*** To protect consumers, it may not be enough for the Services to issue warnings to users who are about to make purchases through third-party app payment methods. Many Americans lack the cyber risk literacy and education needed to avoid falling victim to attractive, low-cost in-app payments embedded with malicious software like ransomware and adware. Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, Pew Research Center (Jan. 26, 2017),

https://pewrsr.ch/3Qkz6nu; *The Risks of Third-Party App Stores*, Norton (Jul. 18, 2018), https://nr.tn/43OqxV0. This is especially true of children and older adults. *See Digital Literacy for Senior Citizens: Building ICT Competencies*, Institute of Electrical and Electronics Engineers (Jul. 18, 2023), https://bit.ly/3KobGJV; Emily A. Vogels and Monica Anderson, *Americans and Digital Knowledge*, Pew Research Center (Oct. 9, 2019), https://pewrsr.ch/3rQJ5qt.

All told, if Plaintiffs' payment processor theory of liability prevails, the Services will have a strong incentive to limit or eliminate payment processing services for apps, and consumers are likely to face serious security risks and be harmed as a result.

## II. AFFIRMING SECTION 230'S ESSENTIAL PROTECTIONS FOR ALGORITHMIC CURATION WILL BENEFIT INTERNET USERS AND APP DEVELOPERS, ESPECIALLY MARGINALIZED SPEAKERS AND AUDIENCES EXPRESSING DISSENT.

One reason that the Internet has become so vital to our everyday lives is that it bolsters the publication of third-party speech at scale, empowering individuals to reach broad audiences based on the strength of their ideas more than any other medium. But the Internet's potential to connect speakers with such audiences is realized only if online platforms are freed from the obligation or incentive to vet the information that individual speakers provide. Section 230 supplies the necessary framework and protections for online platforms to publish third-party speech at their

discretion. 47 U.S.C. § 230(c)(1); *see also* Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 NOTRE DAME L. REV. 33 (2020); JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET, at 1-10 (2019) (same).

This discretionary aspect of publishing embodied in content curation is what makes the Internet valuable to audiences and speakers. Eliminating Section 230 protections that Internet services, including app stores, rely on to curate content would drain the medium of so much of its utility, with particularly dire consequences for marginalized speakers—for example, small app developers—who depend on the Internet to advocate, organize, find community, and make their voices heard.

### A. Section 230's Protections for Content Curation Are Essential to the Basic Functioning of App Stores.

App store operators must have a way to organize the speech that they publish. And given the volume of information on the Services,[3] this organizational process requires automated tools. Online service providers thus employ algorithms to curate content through various methods. *See, e.g.*, Eric Goldman, *Content Moderation Remedies*, 28 MICH. TECH. L. REV. 1, 31-36 (2021) (reviewing a "taxonomy of remedy options"). Some of these methods involve the removal of content, but others

[3] *See, e.g.*, *2022 App Store Transparency Report*, Apple (2023), https://apple.co/3q3cqxk (stating that at the end of 2022, the Apple App Store had 1,783,232 apps); *How Google Play works*, Google, https://bit.ly/3DBAxGy (last visited July 21, 2023) (stating that as of June 2021, Google Play "provides 2 million apps & games to billions of people around the world").

involve reducing the "visibility" of content short of outright removal. *Id.*

Section 230's protections for content promotion and recommendation are essential to this curative process because reducing the visibility of some content on a social media platform necessarily entails the promotion of other content in its stead. There are two reasons for this. *First*, platforms use a process to promote, demote, or remove content: an algorithm programmed to reflect a platform's editorial preferences will rank a given piece of user-generated content against all other content, then use the relative positions of all ranked user-generated content to make publication decisions. *See* Tarleton Gillespie, *Do Not Recommend? Reduction as a Form of Content Moderation*, SOC. MEDIA + SOC'Y, at 6 (July-Sept. 2022) (describing reduction as part of the recommendation process "but flip[ped]"). Only by promoting some content that ranks highly can a platform know to remove or demote other content that ranks lower. *Second*, the promotion of highly ranked content is also the mechanism platforms use to demote low-ranked content or backfill for its removal. *See, e.g.*, Goldman, *Content Moderation Remedies*, *supra*, at 34-35 (discussing this effect).

### B. Withdrawing Section 230's Protections for Content Curation Would Especially Harm Marginalized Speakers and Audiences.

Without Section 230's protections for promoting (and demoting) apps, the Services would be discouraged from supporting vital informational tools. For

example, app store operators could fear that promoting public health and safety information—including information about access to vaccines or the concerns about their use—could expose them to liability. The Services would also become more likely to remove apps that support controversial subject matter. For example, the Services may be unwilling to promote apps that support certain unpopular political views or challenge mainstream opinions for fear of litigation over the content posted on the apps. Or information about reproductive health services could become less available. *See* Letter from Chamber of Progress to Merrick B. Garland, U.S. Att'y Gen. at 2 (Nov. 21, 2022), https://bit.ly/3Ov68jf. Or platforms might exclude pro-Second Amendment apps from their stores to avoid liability for gun violence. The Services would also be discouraged from downranking or hiding apps that support hate speech that they do not condone, such as speech that attacks LGBTQ+ people.

This is no idle speculation. Even when Section 230's protections were selectively withdrawn only as to some kinds of disfavored speech involving sex work, online platforms reacted by shuttering entire portions of their websites to avoid the possibility of being held liable for even still-legal speech. Kendra Albert et al., *FOSTA in Legal Context*, 52 COLUM. HUM. RTS. L. REV. 1084 (2021). Withdrawing Section 230's protections for algorithmic content curation would have comparably nuclear effects for a wide range of disfavored speech and speakers threatened by a patchwork of proscriptive state laws.

Deterring content curation through the greater threat of liability would likewise amplify the volume of risks posed by misinformation, including strategic misinformation deployed by foreign powers seeking to sow discord in the United States. *See* Jack Nassetta & Kimberly Gross, *State Media Warning Labels Can Counteract the Effects of Foreign Misinformation*, HARV. KENNEDY SCH. MISINFORMATION REV. (Oct. 30, 2020) (reporting results of peer-reviewed study showing that content moderation can mitigate the effects of misinformation). Rather than invite protracted litigation over a decision to promote some political statements over others, platforms would not curate political statements at all.

Research also indicates that without protection for their core curation services, some smaller platforms would cease to be economically viable. *See* Jennifer Huddleston, *Competition and Content Moderation: How Section 230 Enables Increased Tech Marketplace Entry*, Cato Inst., at 1-8 (2022), https://bit.ly/47dQaS7; Eric Goldman & Jess Miers, *Online Account Terminations/Content Removals and the Benefits of Internet Services Enforcing Their House Rules*, 1 J. FREE SPEECH L. 191, 209-10 (2021). Because advertisers do not want their advertising to appear alongside spam or other undesired content, and because users do not want to use online services littered with that content, advertising dollars would dry up.

Section 230's protections provide essential scaffolding integral to the modern Internet. Eliminating those protections for app stores that promote or recommend

content would functionally eliminate all of Section 230's protections for app stores, deprive Internet users of the value that app stores provide, and disproportionately harm speakers on society's margins.

## CONCLUSION

For the reasons stated above, the Court should reverse the district court's partial denial of the Services' motions to dismiss and affirm the district court's partial grant of the Services' motions to dismiss.

Respectfully submitted,

Dated: July 31, 2023

*s/ Sean Marotta*
Sean Marotta
Mark W. Brennan
J. Ryan Thompson
Andrew McCardle
HOGAN LOVELLS US LLP
555 13th Street NW
Washington, DC 20004
Telephone: (202) 637-5600

*Counsel for Amici Curiae*
*Chamber of Progress and NetChoice*

Jess Miers
Legal Advocacy Counsel
CHAMBER OF PROGRESS
1390 Chain Bridge Road #A108
McLean, VA 22101

Nicole Saad Bembridge
Associate Counsel
NETCHOICE
1401 K Street NW, Suite 502
Washington, DC 20005

## CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitations of Federal Rule of Appellate Procedure 29(a)(5) because it contains 4,596 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the typestyle requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Office Word for Office 365 in Times New Roman 14-point font.

Dated: July 31, 2023

*s/ Sean Marotta*
Sean Marotta

*Counsel for Amici Curiae*
*Chamber of Progress and NetChoice*

## CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on July 31, 2023. All participants in the case are registered CM/ECF users, and service will be accomplished by the appellate CM/ECF system.

Dated: July 31, 2023

*s/ Sean Marotta*
Sean Marotta

*Counsel for Amici Curiae*
*Chamber of Progress and NetChoice*