Sophia Cope (SBN 233428)
sophia@eff.org
David Greene (SBN 160107)
davidg@eff.org
Aaron Mackey (SBN 286647)
amackey@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

Nicole A. Ozer (SBN 228643)
nozer@aclunc.org
Jacob Snow (SBN 270988)
jsnow@aclunc.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493

Samir Jain (SBN 181572)
sjain@cdt.org
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K Street, NW
Washington, DC 20005
Telephone: (202) 407-8843

Counsel for Amici Curiae Electronic Frontier Foundation, American Civil Liberties Union of Northern California, and Center for Democracy & Technology

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

ETHAN ZUCKERMAN,

Plaintiff,

v.

META PLATFORMS, INC.,

Defendant.

Case No. 3:24-CV-02596-JSC

AMICI CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA, AND CENTER FOR DEMOCRACY & TECHNOLOGY IN SUPPORT OF PLAINTIFF ETHAN ZUCKERMAN

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

A properly broad reading of Section 230(c)(2)(B) is necessary to further the original purpose of Section 230 as a whole: to encourage nongovernmental mechanisms for addressing objectionable online material while not over-promoting censorship by intermediaries. That original purpose remains highly relevant. People who use the internet today desire and need technologies that allow them to control their online experiences.

Section 230 represents an important balance. Sections 230(c)(1) and Section 230(c)(2)(A) offer essential protections for platforms that host third-party content. These provisions create immunity for technology companies moderating content and incorporating blocking and filtering software into their systems. As the internet has grown, technology companies have taken full advantage of these immunities (often with Amici's support). But equally crucial, Section 230(c)(2)(B) provides protection for the development of more expansive technologies, including those (like Unfollow Everything 2.0) developed by third parties, that empower people to have control over their online experiences.

Although Section 230(c)(1)'s immunity for platforms that host user-generated content ultimately benefits individual internet users broadly, Section 230(c)(2)(B) was the mechanism by which Congress gave direct power to individuals, by promoting the development of technologies that allow them to customize their online experiences. Section 230(c)(2)(B)'s immunity for developers of user-empowerment tools is critical for individuals because, while platforms like Facebook can make generalized judgments about "objectionable" material, many such assessments are inherently particular to an individual user and their family. It is vital, then, that the development of technologies that help people control their online experiences and protect themselves from content they find personally objectionable also gets appropriate immunity protection, as the statute directs. Otherwise, the intent of Congress, that Section 230 should support a power balance between what companies can do and what people can control on the internet, is undermined.

Section 230(c)(2)(B) was designed to incentivize and protect technologies like Unfollow Everything 2.0, as well as other tools that help people navigate a complex online environment. The statute helps people act in their own interests, while also advancing worthwhile public policy goals, including privacy and free speech in the modern internet era.

Assuming the truth of the facts as alleged in the Amended Complaint, Unfollow Everything 2.0 is immunized under Section 230(c)(2)(B) from liability for facilitating personal control over the Facebook Newsfeed. Meta's motion to dismiss the complaint should be denied.

ARGUMENT

I. Section 230's Findings, Policy Statements, and Legislative History Confirm That Congress Conferred Immunity on User-Empowerment Technologies

A. Section 230's Findings and Policy Statements Support Granting Section 230(c)(2)(B) Immunity to Unfollow Everything 2.0

Section 230's findings and policy statements themselves articulate that one of the law's primary aims was to facilitate user-empowerment technologies like Unfollow Everything 2.0.

Congress found that people using the internet had the ability to utilize services to exercise "control over the information that they receive" and "the potential for even greater control in the future as technology develops." 47 U.S.C. § 230(a)(2).

Section 230 was meant to "encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services," 47 U.S.C. § 230(b)(3), and to "remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. § 230(b)(4). *See Zango, Inc. v. Kaspersky Lab, Inc*., 568 F.3d 1169, 1174 (9th Cir. 2009) (discussing congressional goals for immunity articulated in Section 230 itself); *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1047 (9th Cir. 2019) (discussing the broad language of Section 230 and the articulated congressional policy goals).

Section 230(c)(2)(B) is an important means to effectuate Section 230's stated policy goal of encouraging the development of technology to empower people to be able to control access to online material. As the Ninth Circuit recognized in *Zango*, "Section 230(c)(2)(B) … covers actions taken to enable or make available *to others* the technical means to restrict access to objectionable material." 568 F.3d at 1174-1175 (emphasis in original).

B. Section 230's Legislative History Supports Granting Section 230(c)(2)(B) Immunity to Unfollow Everything 2.0

The legislative history of Section 230 demonstrates that Section 230(c)(2)(B) was passed to encourage the development of technologies that people could use to control their online experiences, supporting the conclusion that Unfollow Everything 2.0 is the type of tool that Section 230 intended to incentivize and protect against civil suit.

With the rapid development of the internet in the early 1990s, Congress became concerned about sexually explicit material online and its possible access by children.[1] The law that was ultimately passed by Congress in 1996, the Communications Decency Act, incorporated contributions from bills originating in both the Senate and the House of Representatives.

The parts of the law that reflected the Senate's version unconstitutionally imposed speech restrictions on the internet. *See Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) (striking down as unconstitutional sections that criminalized the transmission of "indecent" and "patently offensive" content to children under 18).

What became Section 230(c)(2)(B) originated as part of a House bill that was a direct response to the Senate's governmental censorship approach. Rather than make the transmission of certain content illegal, the House's approach aimed to accomplish similar goals in a manner consistent with First Amendment rights. The Online Family Empowerment Act, also known as the Cox-Wyden Amendment, encouraged non-governmental content moderation and aimed to foster the development of technologies that would enable greater user control. *See* 141 Cong. Rec. H8468 (daily ed. Aug. 4, 1995). As the Ninth Circuit noted, quoting the Congressional Record, "the primary proponents of § 230 in the House stated that they sought to encourage parents to 'get relief now … by … purchas[ing] reasonably priced

[1] *See* 141 Cong. Rec. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Wyden ["[A]s the parents of two small computer-literate children, my wife and I have seen our kids find their way into these chat rooms that make their middle-aged parents cringe. So let us all stipulate right at the outset the importance of protecting our kids…."]), *available at* https://www.congress.gov/crec/1995/08/04/CREC-1995-08-04.pdf. *See id.* at H8471 (statement of Rep. White ["I have got four small children at home. I got them from age 3 to 11, and I can tell my colleagues I get E-mails on a regular basis from my 11-year-old, and my 9-year-old spends a lot of time surfing the Internet on America Online. This is an important issue to me…."]).

software….' 141 Cong. Rec. H8470 (Aug. 4, 1995) (quoting Representatives Cox and Wyden)." *Zango*, 568 F.3d at 1174 n.6 (brackets in original).

Although the specific context in which the overall Communications Decency Act was debated and enacted was related to concern about children's access to sexually explicit material on the early internet, Section 230 was drafted to look beyond those specific concerns as well as the existing technology of the time. As the Ninth Circuit stated, "[a]s more software is developed … users will be able to exercise more control over the content that is transmitted to their computers." *Id.* at 1174.

Section 230(c)(2)(B) was drafted broadly to protect a wide range of user-empowerment technologies like Unfollow Everything 2.0 that support user control. As the Ninth Circuit found, "[T]he conference report goes on to make clear that good [S]amaritan protections apply 'to all access software providers ….' And the definition of access software provider includes any 'provider of software … or enabling tools that … filter, screen, allow, or disallow content.' Therefore, our reading of the text comports with the conferees' expectations." *Id.*

Specific members of Congress agreed that Section 230(c)(2)(B) was intended to spur the development of new tools for people to tailor their online experiences broadly to their preferences. As Representative Goodlatte stated, Section 230 "also encourages the online services industry to develop new technology, such as blocking software." 141 Cong. Rec. H8472 (daily ed. Aug. 4, 1995) (statement of Rep. Goodlatte). Senator Patrick Leahy urged an approach that incentivized user-empowerment technology to address concerns about internet content. *See* 141 Cong. Rec. S10484-86 (daily ed. July 21, 1995).[2] On the House floor, Representative Cox, a co-author of Section 230, discussed that new technology was "quickly becoming available" that would help enable people to "tailor what we see to our own tastes." 141 Cong. Rec. H8470 (daily ed. Aug. 4, 1995) (statement of Rep. Cox).[3]

---

[2] *Available at* https://www.congress.gov/104/crec/1995/07/21/141/119/CREC-1995-07-21-pt1-PgS10484-2.pdf.

[3] Along the same lines, in urging the House-Senate Conference Committee to reject the Senate's version and maintain the House's, Senator Feingold also referenced user-based technology and how the Section 230 provisions both helped "promote the use of existing technology to empower parents to protect their children from objectionable materials on the Internet, and encourages on-line service providers to self-police offensive communications over their private services." 141 Cong. Rec. S27969 (daily ed. Oct. 13, 1995) (Statement of Sen. Feingold), *available at* https://www.govinfo.gov/content/pkg/GPO-CRECB-1995-pt20/pdf/GPO-CRECB-1995-pt20-1-1.pdf.

II. Section 230(c)(2)(B) Advances Public Policy by Supporting the Power of People and Protecting Rights in the Technology Age

A. Section 230(c)(2)(B) Advances User Control Through Delegability

It can be a challenge on the modern internet for people to use online platforms to their full potential and to do so safely. Section 230(c)(2)(B) plays an important role in advancing user control by incentivizing third-party technologies that give people increased functionality that platforms like Facebook may not provide. Section 230(c)(2)(B) effectuates Congress's goal of "maximiz[ing] user control," *see* 47 U.S.C. § 230(b)(3), by supporting the development of user-empowerment technologies like Unfollow Everything 2.0 and thus people's power of delegability—enabling users to "delegate a third-party company, or a piece of third-party software, to interact with a platform on their behalf." [4] This third-party software enables people to better control their online experiences often without requiring any specialized technical skills.

Section 230(c)(2)(B)'s support for third-party tools creates follow-on effects, making a better internet experience for everyone possible. It also benefits technology companies by helping them keep users that would otherwise leave a platform when they are dissatisfied with the available level of user control.

A third-party technology like Unfollow Everything 2.0 relieves people of the binary "stay or leave" choice for platforms like Facebook.[5] This is especially important for those who must use a service because of school, work, community, or other obligations. The power of delegability allows people to make their own choices about their experiences on existing platforms and to stay on those platforms, rather than needing to convince their entire community to migrate to a different platform just to maintain their online connections.

Further, when people can easily alter their online experiences through external tools, and thereby indirectly communicate their preferences to technology companies, this can push the companies to make meaningful changes to improve people's experiences online. When people employ third-party

[4] Bennett Cyphers & Cory Doctorow, *A Legislative Path to an Interoperable Internet*, EFF Deeplinks (July 28, 2020), https://www.eff.org/deeplinks/2020/07/legislative-path-interoperable-internet#delegability.

[5] *See* Cory Doctorow, *Facebook's Secret War on Switching Costs*, EFF Deeplinks (Aug. 27, 2021), https://www.eff.org/deeplinks/2021/08/facebooks-secret-war-switching-costs.

technologies incentivized by Section 230(c)(2)(B), they can thus become co-innovators with platforms, pushing companies attuned to competitive pressures to satisfy these user preferences with new functionalities and means of greater control.

B. Section 230(c)(2)(B) Advances People's Online Privacy

Section 230(c)(2)(B) advances privacy on the internet by incentivizing tools that people use to better control their online experience and block objectionable online material—whether by advertisers, stalkers, or others. *See infra* Part III.

There is a vast power disparity between people and large online services in the modern internet ecosystem. In recent decades, technology companies like Facebook and others have embraced a business model of surveillance capitalism—with profit driven by privacy invasions. [6] Many technology companies engage in widespread collection of information about who people are and what they say and do online. Then they monetize this personal information in various ways: using it to sell behaviorally targeted advertisements, selling the information directly to data brokers,[7] and most recently, using this information to power new artificial intelligence systems.[8] Online behavioral ads can push products that are worse and more expensive.[9] Companies sometimes also target advertisements in a discriminatory manner based on age, sex, race, or ethnicity, resulting in certain groups receiving information about opportunities that others do not.[10] Behavioral advertisements can also be used by outright scammers seeking out financially vulnerable consumers.[11]

---

[6] Shoshana Zuboff, *You Are Now Remotely Controlled*, The New York Times (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html.

[7] Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into The Technology of Corporate Surveillance*, EFF (Dec. 2, 2019), https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance.pdf.

[8] Staff in the Office of Technology and The Division of Privacy and Identity Protection, *AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive*, Federal Trade Commission (Feb. 13, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive.

[9] Eduardo S. Mustri, Idris Adjerid & Alessandro Acquisti, *Behavioral Advertising and Consumer Welfare*, SSRN Electronic Journal (March 23, 2023), http://dx.doi.org/10.2139/ssrn.4398428.

[10] Galen Sherwin & Esha Bhandari, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU (March 19, 2019), https://www.aclu.org/news/womens-rights/facebook-settles-civil-rights-cases-making-sweeping

[11] Bennett Cyphers & Adam Schwartz, *Ban Online Behavioral Advertising*, EFF Deeplinks (March 21, 2022), https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising

The ability for people to use third-party tools helps them navigate the internet while avoiding the pervasive tracking of who they are, where they go, and what they read and watch online.[12] Ad blockers can remove unwelcome ads[13] and protect people from scams and malware.[14] Tracking blockers can stop online entities from placing digital material (often called "cookies") on people's devices that can be used to monitor them across websites.[15]

Additionally, as discussed above in relation to delegability, when people use third-party technologies, they can push companies to start to offer similar tools or reform their practices to become more privacy protective. When people widely adopted the use of third-party ad blockers,[16] companies like Firefox[17] and Brave[18] adopted built-in filtering tools that protect people from online tracking. Presently, Apple is attempting to compete on privacy by highlighting[19] the privacy aspects of its Safari browser.[20]

C. Section 230(c)(2)(B) Respects Free Speech Rights Online

The passage of Section 230 was animated by policymakers' concerns over the effects that the internet could have on people, with a special focus on children. But the law was also carefully crafted to address these issues in a manner that respected free speech rights online.

Other portions of the Communications Decency Act violated the First Amendment by attempting to directly outlaw certain online content. *See Reno*, 521 U.S. at 885. Section 230, however, avoids

---

[12] *Ad Blocker*, PC Magazine Encyclopedia, https://www.pcmag.com/encyclopedia/term/ad-blocker (last visited Sept. 3, 2024).

[13] Tiffany Hsu, *Why Are You Seeing So Many Bad Digital Ads Now?*, The New York Times (Feb, 11, 2023), https://www.nytimes.com/2023/02/11/technology/bad-digital-ads.html.

[14] Zach Whittaker, *Even the FBI Says You Should Use an Ad Blocker*, Tech Crunch (Dec. 22, 2022), https://techcrunch.com/2022/12/22/fbi-ad-blocker/.

[15] Cyphers & Gebhart, *supra* note 7 ("The most common tool for third-party tracking is the HTTP cookie. A cookie is a small piece of text that is stored in your browser, associated with a particular domain.").

[16] Max Eddy, *The Best Ad Blockers for 2024*, PC Magazine (Jan. 11, 2023), https://www.pcmag.com/picks/best-ad-blockers.

[17] Mozilla, *Enhanced Tracking Protection*, https://support.mozilla.org/en-US/kb/firefox-privacy-and-security-features#w_enhanced-tracking-protection (last visited Sept. 3, 2024).

[18] Brave, *Brave Shields*, https://brave.com/shields/ (last visited Sept. 3, 2024).

[19] Juli Clover, *Apple Launches New Safari Ad Campaign: 'A Browser That's Actually Private,'* MacRumors (July 16, 2024), https://www.macrumors.com/2024/07/16/apple-safari-ad-campaign/.

[20] Apple, *Safari & Privacy* (April 6, 2023), https://www.apple.com/legal/privacy/data/en/safari/.

government restrictions on content, and instead provides various immunities to internet users and online services, giving them the legal breathing room to engage in their own content moderation absent government direction. *See generally* 47 U.S.C. § 230(c)(1)(2).

Section 230(c)(2)(B) comports with the First Amendment by incentivizing the development of tools that give people the ability to manage their online experiences outside of government control. As Section 230 itself states: "It is the policy of the United States 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)(2).

Section 230(c)(2)(B) thus promotes tools that are constitutionally preferred alternatives to government censorship. *Cf. Reno*, 521 U.S. at 874, 877 (discussing "user-based software" in the context of "less restrictive alternatives" to the CDA's content bans); *Ashcroft v. ACLU*, 542 U.S. 656, 667 (2004) (holding that "blocking and filtering software" is less restrictive and more effective than COPA). And as the Ninth Circuit recently wrote, affirming that provisions of a California law directed at certain content on the internet failed to pass constitutional muster, "[t]he State could have easily employed less restrictive means to accomplish its protective goals, such as by … incentivizing companies to offer voluntary content filters or application blockers." *NetChoice, LLC v. Bonta*, No. 23-2969, 2024 WL 3838423, at *13 (9th Cir. Aug. 16, 2024).

These cases demonstrate that Section 230 remains, just as it was in the 1990s, an important and constitutional mechanism for addressing concerns about online content.

III. Numerous Technologies Exist to Help People Control Their Online Experiences

Unfollow Everything 2.0 is a prime example of user-empowerment technology that can help people using the internet control their online experiences. Below are a few additional examples.

Social Media Tailoring. Many technologies help people tailor their experiences on social media platforms to their individual content and privacy preferences beyond platform-provided features. Block Party, released in 2022, allowed people using then-Twitter (now X) to "automate the process of blocking

bad actors, trolls, harassers and others."[21] After that technology lost necessary access to Twitter, it relaunched as Privacy Party, allowing people to both understand their privacy risks on social media and configure their privacy settings more easily than the platforms themselves might allow.[22] Ozone allows people using the social media platform Bluesky to review and label content they see on the platform and facilitates actions such as warning people about content that others have found rude or hiding content flagged as spam.[23]

Tracking Blocking. Third-party tools such as web browser extensions allow people to block surreptitious tracking of their online activities particularly in the context of advertising: examples include Privacy Badger (developed and maintained by *amicus* EFF[24]), uBlockOrigin,[25] and Ghostery.[26]

Cyberstalking. Individuals can protect their privacy, safety, and security with third-party blocking and filtering technologies that flag surreptitious tracking software known as "stalkerware," which is often installed on someone's smartphone by a suspicious or vindictive romantic partner.[27]

Digital Security. Technologies keep people's devices and the internet itself secure: antivirus software blocks the installation of malware on individual's devices,[28] while third-party tools like Burp Suite[29] and Wireshark[30] help security researchers identify and address network vulnerabilities by

---

[21] Sarah Perez, *After Losing Access to Twitter's API, Block Party Pivots to Privacy*, Tech Crunch (March 11, 2024, 11:12 AM), https://techcrunch.com/2024/03/11/after-losing-access-to-twitters-api-block-party-pivots-to-privacy/

[22] *Id.*

[23] Bluesky, *Bluesky's Stackable Approach to Moderation*, (March 12, 2024), https://bsky.social/about/blog/03-12-2024-stackable-moderation.

[24] EFF, *Privacy Badger*, https://www.eff.org/privacybadger (last visited Sept. 3, 2024).

[25] *uBlock Origin - Free, Open-Source Ad Content Blocker*, uBlock Origin, https://ublockorigin.com/ (last visited Sept. 3, 2024).

[26] Ghostery, *Privacy You Can See*, https://www.ghostery.com/ (last visited Sept. 3, 2024).

[27] *See* Rebecca Jeschke, *EFF's New "Threat Lab" Dives Deep into Surveillance Technologies—and Their Use and Abuse*, EFF Deeplinks (April 4, 2019), https://www.eff.org/deeplinks/2019/04/effs-new-threat-lab-dives-deep-surveillance-technologies-and-their-use-and-abuse.

[28] *See* EFF, *Antivirus*, Surveillance Self-Defense, https://ssd.eff.org/glossary/antivirus (last visited Sept. 3, 2024).

[29] *See* Port Swigger, *Burp Suite Community Edition*, https://portswigger.net/burp/communitydownload (last visited Sept. 3, 2024).

[30] *See* Wireshark, *The World's Most Popular Network Protocol Analyzer*, , https://www.wireshark.org/ (last visited Sept. 3, 2024).

enabling the filtering of incoming web traffic, thereby protecting both internet networks and the people using them.

Content Sorting. There are tools that help particular communities identify and evaluate certain online speech or forums. Shinigami Eyes, for example, is a browser extension that helps transgender people navigate the internet by highlighting in different colors transphobic and trans-friendly pages and users on most major social network platforms, search engine results, and some other webpages.[31] Third-party filtering technologies like this can help people find safer digital spaces when their identity, expression, or membership in a community carry risks of threats, discrimination, or harassment.

IV. Statutory Text Supports Granting Unfollow Everything 2.0 Immunity Under Section 230(c)(2)(B)

A. Plaintiff is a "Provider of an Interactive Computer Service"

Plaintiff easily fits within the definition of a "provider of an interactive computer service" for purposes of granting him Section 230(c)(2)(B) immunity. An "interactive computer service" is defined, in part, as an "*access software provider* that provides or enables computer access by multiple users to a computer server…." 47 U.S.C. § 230(f)(2) (emphasis added).

First, Plaintiff is an "access software provider" because Unfollow Everything 2.0 is a software tool that enables Facebook users to "filter, screen, allow, or disallow content," "pick" or "choose" content, and "display" or "organize" content, *see* 47 U.S.C. § 230(f)(4), by automating their ability to decide what content they see within their newsfeeds. This is accomplished by the tool unfollowing a users' friends, groups, or pages. The practical effect is to empty out users' newsfeeds and allow them to manually add back any friends, groups, or pages they would like to see in their feeds. [Am. Compl. ¶¶ 52, 60-61, 71, 74]

Second, Unfollow Everything 2.0 "provides or enables computer access by multiple users to a computer server," *see* 47 U.S.C. § 230(f)(2), because (1) users of the tool "will receive updates via the Internet as necessary," (2) users will access Unfollow Everything 2.0's servers to verify the tool works, and (3) users will rely on Unfollow Everything 2.0's servers to communicate with Facebook's servers to execute the unfollowing or re-following. [Am. Compl. ¶¶ 73, 77, Count 1 ¶ 3] [MTD Opp. 14] *See also*

[31] Shinigami Eyes, https://shinigami-eyes.github.io/ (last visited Sept. 3, 2024).

Zango, 568 F.3d at 1173 (holding that "Kaspersky 'provides or enables computer access by multiple users to a computer server' by providing its customers with online access to its update servers").

B. Unfollow Everything 2.0 "Restrict[s] Access" to "Objectionable" Online Material

Plaintiff's Unfollow Everything 2.0 "restrict[s] access" to "objectionable" material consistent with the statutory language of Section 230(c)(2)(B), by allowing Facebook users to effectively create a clean slate on their newsfeed by unfollowing the individuals, pages, and groups that they previously followed, thereby preventing that content from showing up in their newsfeed.

Restricting Access. In interpreting statutes, courts look to the ordinary meaning of statutory terms. *Wooden v. United States*, 595 U.S. 360, 366 (2022). *Accord Eldridge v. Howard*, 70 F.4th 543, 547 (9th Cir. 2023) (citing *Wooden*). In doing so here, "access" is defined as "freedom or ability to obtain or make use of something."[32] And "restrict" is defined as "to confine within bounds."[33]

People who use social media may want to restrict their "ability to obtain or make use of" online material in a wide variety of ways. Some people may want to see certain content immediately, or to see as much of it as possible (it is an internet axiom that some people *really* love cat videos[34]). Other people may prefer to limit what appears automatically compared with requiring them to seek it out, configuring a social media feed in the same way people use rules to filter and categorize email. All of these mechanisms "restrict access" in some way by confining that access "within bounds."

Plaintiff's tool is designed to be used in a similar way—to allow Facebook users to affirmatively restrict their ability "to obtain or make use" of their friends' posted content or any content generated by pages or groups they had followed—within their own newsfeed. [Am. Compl. ¶¶ 52, 60-61, 71, 74]. People who would use Plaintiff's technology desire to have a means to better control what they "obtain or make use of" in their newsfeed. By using this tool, they could not read the content or otherwise interact with it within the newsfeed (for example, by liking it or commenting on it). It is irrelevant, as

[32] Definition of *Access*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/access (last visited Sept. 3, 2024).

[33] Definition of *Restrict*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/restrict (last visited Sept. 3, 2024).

[34] *See* Elizabeth Palermo, *Scientists Explain Why Watching Internet Cat Videos Is Good for You*, NBC News (June 18, 2015), https://www.nbcnews.com/science/weird-science/scientists-explain-why-watching-internet-cat-videos-good-you-n378156.

Defendant argues, that users of the tool may still see their friends' content by proactively navigating to their friends' individual profiles. [*Cf.* MTD 23.] Unfollow Everything 2.0 thus "restrict[s] access" consistent with the statutory terms of Section 230(c)(2)(B).

Objectionable Material. Plaintiff's tool, in allowing Facebook users not to see and interact with their friends' posted content within their newsfeed, easily meets the definition of restricting access to "objectionable" material.[35] The Ninth Circuit has recognized "the breadth of the term 'objectionable'" and rejected the argument that Section 230(c)(2)(B) "cover[s] only material that is sexual or violent in nature." *Enigma Software Group USA*, 946 F.3d at 1051. The court stated, "We think that the catchall was more likely intended to encapsulate forms of unwanted online content that Congress could not identify in the 1990s." *Id.*

This interpretation allows users of Plaintiff's tool to customize their Facebook experiences according to their preferences rather than only to what Congress deems "objectionable." This broad reading of "objectionable" is necessary for Section 230(c)(2)(B) to fulfill its intended goal of promoting a personalization of online services that is impossible at the platform level. What is objectionable to one person may be completely acceptable to another person, whether that is a broad category of online material, or only a certain example of it.

C. The Scope of Section 230(c)(2)(B) is Textually Limited

By its terms, Section 230(c)(2)(B)'s immunity would *not* apply to technologies that weaken user control by engaging in data practices that might, for example, violate privacy laws. [*Cf.* MTD 18.] Such actions would be outside the scope of the immunity. Section 230(c)(2)(B)'s language already limits the immunity for third-party tools only to functions that restrict access to online material. Section 230(c)(2)(B) states that providers of user-empowerment tools have immunity when they are sued "*on account of* any action taken to enable or make available … the technical means to restrict access" to objectionable material. 47 U.S.C. § 230(c)(2)(B) (emphasis added). Thus, per the text of the statute, software features that do not restrict access to objectionable material are not entitled to Section

[35] The Ninth Circuit concluded "that the reference to the 'material described in paragraph (1)' is a typographical error, and that instead the reference should be to paragraph (A)." *Zango*, 568 F.3d at 1173 n.5.

230(c)(2)(B) immunity. *Zango*, 568 F.3d at 1176 (discussing "non-filtering programs" as outside of the immunity).

V. Congress Did Not Intend to Allow Online Services to Block Section 230(c)(2)(B)'s Immunity By Rewriting Their Terms of Service

Section 230(c)(2)(B) does not include an exception for contract claims (like violations of Meta's Terms of Service) because it would defeat the whole purpose of the immunity.

Section 230(c)(2)(B)'s broad immunity for third-party tools recognizes that users would deploy such tools to directly interact with online services at the users' direction. And as explained above, *see supra* Part II, platforms do not always prioritize their users' interests in having a customizable experience online, and user-empowerment tools often fill these gaps. Congress did not create an immunity that could so easily be evaded by crafting Terms of Service that prohibit the application of blocking and filtering technologies to companies' online services.

This Court thus should not endorse Meta's contract argument because the result would render Section 230(c)(2)(B)'s immunity wholly ineffectual and irrelevant. In Meta's preferred world, Meta could wield a Facebook TOS violation—which the company has total control over—like a cudgel and deter any technology like Unfollow Everything 2.0 from ever being used by Facebook users. That would chill the innovative marketplace for user-empowerment tools, as new entrants would avoid the legal risk of having to fight Meta's contract lawsuits, despite Facebook having the single largest user base of any social media service on the planet.[36]

Meta's contract argument is also incorrect as a matter of law for at least two reasons.

First, no court has interpreted Section 230(c)(2)(B)'s immunity as including, *sub silentio*, an exception for contract claims. [*See* MTD Opp. 17-18.] The Ninth Circuit cases at the heart of Meta's argument concern the scope of immunity Congress conferred under Section 230(c)(1), not Section 230(c)(2)(B). *See Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1109 (9th Cir. 2009) (holding that plaintiff's promissory estoppel claim against Yahoo! for failing to take down fraudulent profiles of plaintiff was not barred by Section 230(c)(1) but expressly declining to examine Section 230(c)(2)). *See also Calise v.*

[36] *See* Stacy Jo Dixon, *Most Popular Social Networks Worldwide as of April 2024, By Number of Monthly Active Users*, Statista (July 10, 2024), https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

Meta Platforms, Inc., 103 F.4th 732, 743 (9th Cir. 2024) (holding that plaintiff's contract claims against Meta for failing to take down "scam advertisements" were not barred by Section 230(c)(1)). In fact, the Ninth Circuit opined that Section 230(c)(2) provides immunity against contract claims "premised on the taking down of a customer's posting…." *Batzel v. Smith*, 333 F.3d 1018, 1030 n.14 (9th Cir. 2003).

Second, *Barnes* and *Calise* stand for the proposition that when a platform promises to engage in some conduct unrelated to its status as a publisher of user-generated content, Section 230(c)(1) does not confer immunity on that unrelated promise. *See Calise*, 103 F.4th at 743. *See also Barnes*, 570 F.3d at 1107. *Cf. Brittain v. Twitter, Inc.*, No. 19-CV-00114-YGR, 2019 WL 2423375 , at *4 (N.D. Cal. June 10, 2019) (holding that plaintiff's breach of contract claim premised on Twitter having suspended his accounts was barred by Section 230(c)(1) because it sought to treat Twitter as a publisher). To the extent that *Barnes* and *Calise* may be relevant to Section 230(c)(2)(B), they confirm that when the promisor-defendant is the *developer of a user-empowerment tool* (rather than the platform, as in those cases), such developers are immune from contract claims brought by platforms that arise out of the technology's conduct of blocking or filtering online material at the direction of users. Unfollow Everything 2.0 and similar user-empowerment tools are not engaging in any separate conduct or undertaking any separate promises *outside of* blocking or filtering online material. [*See* MTD Opp. 17 ("Some breach-of-contract claims might not be based on actions taken to enable filtering, of course, and those claims could proceed against a defendant that otherwise satisfied section 230(c)(2)(B).")]

If Meta could simply amend its Terms of Service to prohibit tools contemplated by Section 230(c)(2)(B), Meta would have complete control over how people use their product. That may be what Meta wants, but Section 230(c)(2)(B) provides otherwise.

CONCLUSION

For the above reasons, the Court should find that Plaintiff's Amended Complaint alleges facts that entitle him and his Unfollowing Everything 2.0 technology to immunity under Section 230(c)(2)(B), and the Court should deny Meta's Motion to Dismiss.

Dated: September 5, 2024

Respectfully submitted,

By: /s/ *Sophia Cope*

Sophia Cope (SBN 233428)
David Greene (SBN 160107)
Aaron Mackey (SBN 286647)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Email: sophia@eff.org, davidg@eff.org, amackey@eff.org,

Nicole A. Ozer (SBN 228643)
Jacob Snow (SBN 270988)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Email: nozer@aclunc.org, jsnow@aclunc.org

Samir Jain (SBN 181572)
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K Street, NW
Washington, DC 20005
Telephone: (202) 407-8843
Email: sjain@cdt.org

Counsel for Amici Curiae Electronic Frontier Foundation, American Civil Liberties Union of Northern California, and Center for Democracy & Technology