Statement of Professor Eric Schnapper

I.

Section 230(c)(1) was adopted for the purpose of distinguishing between conduct of third parties and conduct of internet companies themselves. Its familiar language provides that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by *another* information content provider." The last four words are central to the limitation on the defense created by the statute; it is only regarding information created by "another" that the defense may be available. Section 230(e)(3) makes clear that even a partial role played by an internet company in the creation of harmful material would fall outside the protections of the statute. Section 230(f)(3) defines the term "information content provider" as "any person or entity that is responsible, in whole or *in part*, for the creation or development of information provide through the Internet or any other interactive computer service."

The legislative history of the statute makes clear that Congress enacted the law because it believed it would be impossible for internet companies to prevent all harmful materials from being posted on their websites, and that it would be unfair to hold them responsible for what was posted there by others, at least if they did not know what was being posted. Representative Lofgren explained the imposing strict liability on an internet company for unknown materials on its website would be "like saying that the mailman is going to be liable when he delivers a plain brown envelope for what is inside it." 141 Cong. Rec. 22046 (1996). Representative Goodlatte made the same point:

> There is no way that any of those entities, like Prodigy, can take the responsibility to edit information that is going to be coming in to them from all manner of sources onto their bulletin board. We are talking about something that is far larger than our daily newspaper. We are talking about something that is going to be thousands of

> pages of information every day, and to have that imposition imposed on them is wrong.

141 Cong. Rec. 22046.

Congress acted in reliance on representations that there was no way for internet companies to exhaustively monitor the content of all the material that was being posted. "We have been told it is technologically impossible for interactive service providers to guarantee that no subscriber posts indecent material on their bulletin board services." 141 Cong. Rec. 22046 (remarks of Rep. Goodlatte).

The focus of this concern was expressly restricted to limiting liability for actions by other parties. Thus Representative Goodlatte's comments were about what a "subscriber posts," and about what is "coming in to" internet companies. In Representative Lofgren's hypothetical, the letter carrier was not responsible for whatever someone else had placed in the "plain brown envelope." Both Member of Congress assumed that the role of the internet company would be a limited one; permitting the posting of material "onto [its] bulletin board," or "deliver[ing]" that material to whatever location had been chosen by whoever addressed the envelope.

That account made complete sense in the context of the most common websites of the era when § 230(c)(1) was enacted. The legislative history focused on the three largest websites used by ordinary consumers of that time: Prodigy, CompuServe, and America Online, none of which still exists except in vestigial form. Regarding third-party content, those websites of yesteryear were essentially passive. Users could post material on the websites, or obtain material from it, but the role of the website itself was largely limited to providing structured locations within the website to which materials could be posted or where those materials could be found. Because of the economics of those websites—they charged monthly fees to users—they usually had no interest in increasing the amount of usage by a particular user. In fact, due to limited capacity they were

incentivized to tamp down time spent by users on their sites. Under the monthly fee structure the ideal user was one who utilized the website very little. Indeed, reports from that era were concerned that the increasing use and popularity of websites threatened to overwhelm their technical capacity.

In *Reno v. American Civil Liberties Union,* 521 U.S. 844 (1997), decided shortly after the enactment of § 230(c)(1), the Supreme Court provided a description of the relationship between users and websites in which, with the exception of a search engine, the website itself did nothing at all.

> A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.
>
> From the publishers' point of view, it constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals. Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege.

521 U.S. at 852-53 (footnote omitted).

Consistent with the text of the statute, and with its original purpose, courts have repeatedly described the defense created by section 230(c)(1) as inapplicable to conduct engaged in by the website itself.[1]

II.

Within a decade of the enactment of section 230(c)(1), there was a fundamental change in the financial basis of the major consumer website companies, a change which has led those companies to engage in an increasing amount of activity of their own. By the early years of this century, access to the internet was no longer based on subscription-based (and, previously, dial-up) services. Individuals largely accessed the internet through high-speed connections provided cable companies or other local providers. And, critically, the major internet companies that emerged and thrived based their revenues, not on monthly subscriptions, but on advertising.

For an advertisement-revenue-based internet company, the main basis of its income and financial success is the amount of time that users spend on the firm's website; the longer a user is on a website, the more advertisements he or she can be shown, and the more revenue the company will receive. Thus, for these companies, the central task of their business is to find ways to persuade users to spend as much time as possible looking at materials on their websites. Few firms, if any, have been content to hope that third parties will post materials that potential users will find

[1] *Henderson v. Source for Public Data*, 53 F.4th 110, 126 (4th Cir. 2022) ("Public Data's own actions"); *Fair Housing Council of San Fernando Valley v. Roomates.com, LLC*, 521 F.3d 1157, 1169 n. 24 (9th Cir. 2008) ("their own conduct"); *Federal Trade Commission v. LeadClick Media LLC*, 838 F.3d 158, 171 (2d Cir. 2016) ("LeadClick's own actions"); *Lemon v. Snap, Inc*., 995 F.3d 1085, 1093 (9th Cir. 2021) ("its own conduct") (quoting *Maynard v. Snapchat, Inc*., 346 Ga. App. 131, 816 SE 2d 77, 81 (2018)); *Webber v. Armslist LLC*, 572 F. Supp. 3d 603, 616 (E.D. Wisc. 2021) ("their own misconduct"); *Lee v. Amazon.com, Inc*., 76 Cal. App. 5th 200, 257, 291 Cal. Rptr. 322, 377 (Ct. App. 1st Dist. 2022) ("Amazon's own conduct"); *Massachusetts Port Authority v. Turo, Inc*., 487 Mass. 235, 243 (2021) ("Turo's own conduct").

interesting, or to simply wait until users at their own initiative ask to see a particular video, tweet, or text. Rather, the focus of much of the activity of most advertisement-revenue-based websites is to devise automated strategies of their own—typically relying on algorithms—to promote and increase such usage.

Targeting using algorithms has been central to these promotional efforts of websites. Most websites have a wide variety of users. Efforts to promote the same third-party content to all users would often be ineffective; a prominently displayed thumbnail about a cooking video on YouTube's home page would be unlikely to interest users primarily concerned with sports, pets, current events, travel, fashion, or archeological discoveries. Instead, major websites collect copious amounts of data about users, and rely on what they know about each user, including information about which materials he or she has viewed in the past, how long was spent viewing it, how often a particular user follows up with more videos on similar subjects, etc., to select the particular material to recommend. Working in the background, the internet company's algorithm develops an ever-more-detailed, and constantly updated and pruned, profile of each user. The algorithms are constantly being tweaked to result in longer viewer engagement by targeted users; some of those ongoing adjustments are made directly by software engineers, and some by artificial intelligence software which monitors the ways in which users have responded to past recommendations.

Most Americans have experienced the effectiveness of these algorithms in the context of promoting advertising. As one uses a website like YouTube, Facebook, TikTok, etc., those sites show the Used in this manner, the algorithms allow advertisers to laser-focus their advertisements on particular micro-demographics. This can also create problems, such as when a housing

developer focuses real estate listings on a demographic profile that excludes particular racial groups.

The internet companies use similar algorithms to induce users to remain on their websites longer so they will view more of these targeted advertisements. The manner in which websites seek to induce users to look at particular materials, and to remain on the website (and available for advertising) for as long as possible, vary widely, and are continuing to evolve. Officials in these companies generally refer to these practices as "recommendations," although that is not a term in § 230(c)(1) itself and has no fixed meaning in either the law or in industry usage. Today those promotional practices, taken at the initiative of the website itself, rather than in response to some request from a user, include the following:

> *Displaying unrequested videos, pictures or text*—Once a user looks at a particular item, or selects a type of material, the website displays a continuous series of materials, materials generally chosen by the website's algorithm to maximize the likelihood that the user will continue to watch whatever the website has selected. Autoplay in YouTube is such a feature, and much of what occurs on TikTok and Instagram functions that way.
>
> *Displaying advertisements for promoted material*—Websites may proffer to a user what are in effect a targeted set of advertisements for material available on the website itself. The thumbnails that a user sees on YouTube are usually chosen in that manner, as are the snippets of text that appear on Feed (formerly News Feed) on Facebook. A URL (usually created by the website itself) is embedded in each thumbnail or snippet, so that a user can easily access the promoted material. On Facebook pictures of possible new individuals to "friend" function in this manner.

Promotional language—Websites sometimes include words or information of their own to encourage users to select particular materials, terms such as "trending," or "you might like," or data about the number of likes or views.

Notifications—Websites may send push notifications, text messages or emails to viewers announcing newly available materials, or post such announcements on a page a user will visit.

Autocomplete—TikTok includes a feature that tends to direct users to particular content by automatically completing search terms as the user starts to type them. According to a complaint recently filed by the Indiana Attorney General, that feature often directs users to materials about drugs and sexual materials inappropriate for minors. The complaint alleges, or example, if a user types "shr" into the TikTok search bar, TikTok suggests "shroomz" as a possible search term, which leads the viewer to materials about hallucinogenic mushrooms.

These various website promotional practices have, overall, been extremely effective. YouTube officials, for example, estimate that about 70% of the views on its website are a result of its recommendations.[2]

III.

Although these promotional practices have been quite lucrative, they also have resulted in streams of increasingly harmful materials being directed at users. Evaluations of the distribution

[2] YouTube's Recommendations Drive 70% of What We Watch," available at qz.com/1178125/youtubes-recommendations-drive-70- of-what-we-watch, visited Nov. 16, 2022.

of terrorist and other extremist materials have concluded that most of those distributions is a result of website algorithm-based targeted promotional practices.

In 2019-20, a researcher employed by Facebook created an account for a fictional user named Carol Smith. The fictional Smith described herself as a politically conservative mother from North Carolina, with an interest in politics, Fox News, and then-President Trump. Although that description did not express an interest in conspiracy theories, within two days the Facebook algorithms were recommending that she join groups dedicated to QAnon. Within a week, Smith's feed was full of groups and pages that violated Facebook's nominal rules, including those against hate speech. That study, entitled "Carols's Journey to QAnon," and other Facebook studies that showed test users receiving a "barrage of extreme, conspiratorial and graphic content," have ben provided to Congress in redacted form by Frances Haugen.

In 2022 a study of YouTube yielded a similar result. An Arabic language search for the term "Jews" and for the name of a Hamas official soon led to videos lauding suicide bombings, and containing antisemitic rhetoric about the Rothschild family.[3]

A number of analyses have suggested that this occurs because website algorithms have concluded that exposing users to more extreme content is likely to result in longer periods of viewing of the website in question. The large amount of information that websites often have about individual users makes these practices especially effective in radicalizing users and recruiting terrorists. If YouTube posted ISIS recruiting videos on a website shown to everyone who visited YouTube, the overwhelming majority of viewers would simply be horrified. But YouTube has,

[3] Brief of Amici Curiae Major General Tamir Hayman, *et al*., Gonzalez v. Google LLC, No. 21-1333, at 27-28

and uses, the ability to identify and target the particular individuals likely to watch terrorist or extremist videos, an ability which the terrorist or domestic extremist groups themselves lack.

When websites first began to engage in promotional practices, they could have chosen to limit such recommendations to a carefully screened group of videos, texts, and tweets. Or, recognizing that this use of recommendations bears no relationship to the passive role that § 230(c)(1) was adopted to protect, internet firms could have asked that Congress to amend the statute. Instead, those firms simply swept into their recommendation functions whatever was on their websites. Thus the affirmative promotion of terrorist or other extremist material has followed inexorably from the failure of websites to identify and remove those materials in the first place.

The consequences of these practices for national security have been exceptionally serious. In the *Twitter, Inc. v. Taamneh* litigation, a group of retired United States generals, including first commander of Operation Inherent Resolve in Iraq and Syria, explained that:

> social media played a central role in making [ISIS], at least for several years, the most successful and most viscous terrorist group in modern history,… ISIS[‘s]…massive recruitment effort, carried out to a significant degree through the [Twitter, Facebook and YouTube]’s social media platforms, is one key to ISIS’s initial success.[4]

Other Defense Department officials pointed out that:

> ISIS has used [social media] platforms to exhibit intimidation, networking, recruitment, justice, and justification…. The group has embraced social media as a weapon of war, using it to spread official messages, recruit, fundraise, and network.[5]

[4] Brief of Amici Curiae Retired United States Generals, *Twitter, Inc. v. Taamneh*, 3-4 (emphasis omitted).

[5] Heather Marie Vitale and James M. Keagle, “A Time to Tweet, as Well as a Time to Kill: ISIS’s Projection of Power in Iraq and Syria, Defense Horizons,” Nat’l Defense Univ. 1, 6 (Oct. 2014).

While this subcommittee meets to discuss website promotional practices, several thousand members of the United States armed forces remain in harm's way on the ground in Syria and Iraq dealing with the consequences of those actions.

For decades social media platforms have steadily become overrun with hate speech, incitement to terrorism, domestic violence, and calls for antisemitic violence. The refusal of social media platforms to implement effective steps of self-regulation have resulted in the murder of Nohemi Gonzalez, Mehier Taamneh, and many other innocent victims worldwide. While the social media platforms have to flourished and prospered, the safety of the American public and other communities worldwide has been imperiled as terrorists are provided use of this powerful tool to carry out their deadly attacks. Congress never intended section 230 to provide a defense for internet companies when their own conduct causes such grievous harms.

In August and September 2014, American journalists James Foley and Steven Soloff were beheaded by ISIS, horrific events videotaped and publicized by their killers. Two months later, a spokesman for Twitter, in explaining why Twitter still was not removing ISIS from its platform, explained "[o]ne man's terrorist is another man's freedom fighter."[6] Those extraordinary eight words are a compelling demonstration that absolute immunity can breed absolute irresponsibility. This subcommittee will doubtless be assured that that attitude has changed. But as recent events have made all too clear, in the absence of any legal consequences for policies based on that attitude, and as long as websites can wield § 230(c)(1) like a human shield to protect their own conduct, any existing website policy could be swept away with the next change in ownership or personnel.

[6] Jenna McLaughlin, "Twitter Is Not at War With ISIS. Here's Why," MOTHER JONES (Nov. 18, 2014).