Senate Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law
Hearing on Platform Accountability: *Gonzalez* and Reform

Testimony of Dr. Mary Anne Franks
Michael R. Klein Distinguished Scholar Chair and Professor of Law, University of Miami
President and Legislative & Tech Policy Director, Cyber Civil Rights Initiative
March 8, 2023

I. Introduction

In the Biblical parable of the Good Samaritan, a traveler is beaten by robbers and left half dead by the side of the road. A priest sees him but passes by without stopping; a Levite later does the same. Finally, a man from Samaria comes upon the injured traveler. He stops, tends to the man's wounds, and takes him to an inn to receive further care. "Good Samaritan" laws, which exist in every state, commonly provide legal protection to individuals who, like the Good Samaritan in the Bible story, voluntarily attempt to assist others in need.

In 1996, Congress passed a "Good Samaritan" law for the internet: Section 230 of the Communications Decency Act. The law's operative provision is titled "Protection for 'Good Samaritan' blocking and screening of offensive material." Legislative headings supply important guidance about a provision's intended meaning, providing "a short-hand reference to the general subject matter" to which Congress meant to apply the provision.[1] Section 230 (c)(2) spells out the significance of the provision's title, expressly offering immunity from civil liability to providers and users of interactive computer services (such as search engines and social media platforms) for actions "voluntarily taken in good faith to restrict access to or availability of" objectionable content.

For more than twenty years, however, most courts have ignored the text and history of Section 230 and instead interpreted this online Good Samaritan law to protect not only Internet sites and services that attempt to restrict harmful content, but also those that make no effort to restrict access to harmful content. Worse still, some courts have even interpreted the law to protect those who *solicit* harmful content, *amplify* it, and even *profit* from it. In this upside-down version of the Good Samaritan parable, not only indifferent priests and Levites, but also enterprising passersby who point crowds to the bloody spectacle for a price, are granted the same protections as the Good Samaritan. In other words, courts have treated Section 230 not as the Good Samaritan law that Congress enacted, but as a Bad Samaritan law that rewards reckless, unaccountable, and destructive online behavior.

The consequences of granting this carte blanche, unqualified immunity to large social media companies and other online platforms are entirely predictable. Harmful content flourishes online, causing grave and lasting injury to vulnerable communities, even when those harms are clearly foreseeable and easily preventable. Sites devoted to nonconsensual pornography, commonly known as "revenge porn," can operate without fear of liability for the devastating social,

[1] Trainmen v. Balt. & Ohio R.R. Co., 331 U.S. 519, 528 (1947).

emotional, and economic harms caused by allowing users to post intimate images of others without their consent. Social media platforms that host forums for the radicalization of bigots and misogynists can avoid any legal responsibility for the online abuse and doxing on their sites directed at vulnerable groups. And the online gathering places for the darkest and most destructive conspiracy mongering enjoy blanket immunity when their sites are used to harass and terrorize election officials or victims of gun violence.

Perpetuating this kind of Bad Samaritan immunity is especially egregious considering how the Internet and social media platforms can exacerbate and magnify the harms of abuse and harassment. The anonymity provided by many social media platforms allows the perpetrators of abuse to avoid detection. The reach and amplification of social media allow abuse to be crowdsourced and broadcast to a wide audience. And the permanence of online content means that harmful content or private information can be nearly impossible to remove from public view. All of this contributes to the virtual captivity in which online abuse permeates every aspect of the victim's life, and opportunities to escape from the global reach of technology are extremely limited. It is therefore no wonder that online abuse has serious consequences for victims' freedom of expression, professional and educational opportunities, civic participation, and mental health.

II. *Gonzalez v. Google* (2023)

On February 21, 2023, the Supreme Court took up the question of the proper scope of Section 230 for the first time. *Gonzalez v. Google* presents the Court with the question of whether Section 230 provides immunity to Google for allegedly using targeted algorithms to promote violent extremist video content. Some critics of the tech industry have argued that the use of targeted algorithms can never be protected by Section 230 immunity, while tech industry supporters claim that the use of targeted algorithms should always warrant Section 230 immunity.

Both of these positions are wrong. Targeted algorithms are one of the most effective tools that online platforms and services can use to restrict harmful content, which is exactly the kind of action that Section 230 immunity is intended to protect. But Google's alleged actions in this particular case *amplified* rather than restricted access to terrorist propaganda. For that reason, the company should not receive Section 230 immunity.

During oral argument in Gonzalez, Justice Ketanji Brown Jackson correctly explained Section 230's text, history, and purpose as a Good Samaritan statute. As such, its primary goal is to incentivize voluntary, good faith interventions against harm. The "unqualified immunity" interpretation of Section 230 erases that incentive to help, and in fact provides an incentive to harm – tech companies can act as recklessly as they want in designing their products and services, because more harmful, provocative content equals more profit.

Defenders of the Section 230 status quo often claim that any restriction in the scope of protection makes online intermediaries legally responsible for everything users post on their platforms. But the absence of immunity is not the same thing as the presence of liability. The bystander who fails to help a robbery victim does not enjoy the benefit of Good Samaritan immunity, but this

does not mean the bystander is legally responsible for the robbery. It is only when and if that bystander not only fails to help, but actively causes harm—for example, by taking photos of the victim to distribute for profit—that they could and should face potential liability for that harm.

A slightly more sophisticated version of this objection maintains that the risk of liability – the mere *possibility* of being sued – will force tech companies to take down any third-party content that could be controversial, resulting in the loss of valuable, First Amendment-protected expression. But as Justice Elena Kagan noted during the *Gonzalez* oral argument, "every other industry has to internalize the costs of its conduct. Why is it that the tech industry gets a pass?" Auto manufacturers can be sued when engines catch on fire; cigarette companies can be sued when smokers get lung cancer; hospitals can be sued for botched surgeries. But cars still get made, cigarettes keep being sold, and doctors still operate. There is no reason to think that allowing people to sue when they are harmed by a product means that the product will cease to exist in any meaningful sense. Indeed, the potential for litigation is often a powerful motivator for industries to become safer, more efficient, and more innovative.

Some argue, however, that the Internet is fundamentally different from cars and cigarettes and hospitals because the product in question is speech, and speech deserves special protection under the First Amendment. It is first important to note that the way that Section 230 is currently interpreted shields far more than speech protected by the First Amendment – everything from defamation to credit card transactions to sales of illegal firearms. People use the Internet for a vast array of activities that are not "speech" in any First Amendment sense: paying bills, selling stolen goods, shopping for dog leashes, booking hotel rooms, renewing driver's licenses. The fact that Section 230 uses the term "information" rather than "speech" has helped tech platforms invoke the law to absolve themselves of responsibility for virtually everything individuals do online – a protection that goes far beyond anything the First Amendment would or should protect.

Second, the tech industry is not the only speech-focused industry. Colleges and universities are very much in the business of speech, but they can be sued for discrimination and harassment. So can book publishers and book distributors, radio stations, newspapers, and television companies. The New York Times and Fox News have no special, sweeping immunity from liability the way the tech industry does; indeed, the *New York Times* was sued just last year by Sarah Palin for defamation and the Fox Corporation is currently being sued for defamation by Dominion Voting Systems. The newspaper and television industries have not collapsed under the weight of potential liability, nor can it plausibly be argued that the potential for liability has constrained them to publishing and broadcasting only anodyne, non-controversial speech.

Of course, some calls for tech industry liability do indeed threaten free speech. Some of the most pernicious attacks on free speech and the First Amendment in recent years have come in the guise of Section 230 reform. While it may be easy to forget, social media platforms are private entities with their own First Amendment rights of speech and association. It is vitally important to respect those rights and to reject any attempt by government actors to force social media platforms to carry certain speech or demand that they provide access to certain speakers. Respecting free speech and the First Amendment means respecting tech companies' right to fact-check, label, remove, ban, and make other interventions as they see fit about the content on their

sites. Providing additional or alternative information to false or misleading posts is classic "counterspeech," a treasured First Amendment value. The First Amendment also protects the right to refuse to host content altogether, as the right to free speech includes both the right to speak and the right *not* to speak. As the Supreme Court held in *West Virginia State Board of Education v. Barnette*, "If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion, or force citizens to confess by word or act their faith therein."[2] The First Amendment also protects the right of association, including the right of private actors to choose with whom they wish to associate.[3] And the Supreme Court has long recognized that private-property owners generally have the right to exclude individuals from their property as they see fit.[4]

But allowing tech companies to enjoy unqualified immunity for everything they promote and profit from inflicts economic, physical, psychological and free speech harms. Those targeted for abuse shut down social media profiles and withdraw from public discourse. Those with political ambitions are deterred from running for office. Journalists refrain from reporting on controversial topics. While the current model shielding the tech industry from liability may ensure free speech for the privileged few, protecting free speech for all requires legal reform.

In deciding *Gonzalez*, the Supreme Court has the opportunity to correct the misreading of Section 230 that has plagued the lower courts for decades and allow it to operate as the kind of Good Samaritan law that Congress originally enacted. If the Court does so, victims of online abuse may finally be able to seek justice against platforms who have contributed to their injuries. And, in turn, platforms may finally recognize the value of taking affirmative measures to curb abuse and protect users.

III. Reform Recommendations

But the Supreme Court may also decide that the task of establishing the proper scope of Section 230 immunity is best left to Congress. As Justice Kagan observed, "we're a court. We really don't know about these things. You know, these are not like the nine greatest experts on the Internet."

If the Supreme Court fails in *Gonzalez v. Google* to scale back the excessively broad interpretation of Section 230 that has taken hold in the courts, Congress should take up the responsibility of amending Section 230 to clarify its purpose and foreclose interpretations that render the statute incoherent. At a minimum, this means two specific changes: amending the statute to make clear that interactive computer service providers that demonstrate deliberate indifference to harmful content are ineligible for immunity; and making clear that the law's protections apply only to speech.

2. 319 U.S. 624, 642 (1943).
3. *NAACP v. Alabama ex rel. Patterson,* 357 U.S. 449 (1958).
4. *PruneYard Shopping Ctr. v. Robins,* 447 U.S. 74, 82 (1980).

To accomplish the first change, Section 230 (c)(1) should be amended to state that providers or users of interactive computer services cannot be treated as the publisher or speaker of speech *wholly provided by* another information content provider, *unless such provider or user intentionally encourages, solicits, or generates revenue from the speech, or exhibits deliberate indifference to harm caused by that speech.*

To accomplish the second change, the word "information" in Section 230 (c)(1) should be replaced with the word "speech." This revision would put all parties in a Section 230 case on notice that the classification of the content at issue as protected speech cannot be assumed, but instead must be demonstrated. If a platform cannot make a showing that the content or information at issue is speech, then it should not be able to take advantage of Section 230 immunity.

As important a Section 230 reform is, however, it is not a silver bullet for the wide-ranging harms facilitated by the tech industry. Congress should also enact narrowly targeted federal criminal legislation to address new and highly destructive forms of technology-facilitated abuse, especially those disproportionately targeted at vulnerable groups, including nonconsensual pornography, sexual extortion, doxing, and digital forgeries ("deep fakes"). As Section 230 immunity does not apply to violations of federal criminal law, the creation of these laws will ensure that victims of these abuses will have a path to justice with or without Section 230 reform.

Congress should finally pass the Stopping Harmful Image Exploitation and Limiting Distribution (SHIELD) Act, which would make it a crime to knowingly distribute or threaten to distribute private, sexually explicit visual material of an individual with knowledge of or reckless disregard for the depicted individual's lack of consent to the distribution and reasonable expectation of privacy and without a reasonable belief that distributing the depiction touches a matter of public concern.[5] Congress should also pass a measure similar to the Online Safety Modernization Act of 2017, sponsored by Congresswoman Katherine Clark, which would prohibit multiple forms of "cybercrimes against individuals" including both sextortion and doxing.[6]

Congress should also enact legislation, including criminal legislation, to regulate information that involves verifiably false information that is likely to cause significant harm. Such legislation should include the criminalization of digital forgeries (colloquially known as "deep fakes"). The definition of digital forgeries should be limited to audiovisual material that has been created or materially altered to falsely appear to a reasonable observer to be an actual record of actual speech, conduct, appearance, or absence of an individual, which is created, distributed, or reproduced with the intent to seriously harm or with reckless disregard for whether serious harm

[5] H.R.6998. The SHIELD Act, for which I served as the primary drafter, came very close to becoming law in 2021, when it was included in the House version of the Violence Against Women Reauthorization Act of 2021 but omitted from the Senate version, and again in 2022, when it was included in the omnibus spending bill but removed by Republican leadership at the last moment. *See* Danielle Campoamor, *What it's like to be a victim of 'revenge porn' as a mom: 'It broke my heart,'* Today (Jan. 5, 2023), https://www.today.com/parents/moms/revenge-porn-victims-are-also-moms-speak-rcna62093

[6] H.R.3067.

would result to a falsely depicted individual, or with the intent to incite violence or interfere with official proceedings.

IV. Conclusion

At the most fundamental level, the current problem with the tech industry is the lack of incentive to behave responsibly. The preemptive immunization from liability that courts have interpreted Section 230 to provide means that the drive to create safer or healthier online products and services simply cannot compete with the drive for profit. As long as tech platforms are allowed to enjoy all of the benefits of doing business without any of the burdens, they will continue to move fast and break things, and leave average Americans to pick up the pieces.

The unqualified immunity interpretation of Section 230 creates what economists call a moral hazard: when an entity is motivated to engage in increasingly risky conduct because it does not bear the costs of those risks. The devastating fallout of that moral hazard is all around us: an online ecosystem flooded with lies, extremism, racism, and misogyny that is fueling offline harassment and violence.