NetChoice *Promoting Convenience, Choice, and Commerce on The Net*

NetChoice

Carl Szabo, Vice President and General Counsel 1401 K St NW, Suite 502 Washington, DC 20005 202-420-7485 www.netchoice.org

July 6, 2021

RE: Opposition to AB 587

We respectfully ask that you not advance AB 587, because it:

- Impedes the ability of platforms to remove terrorist recruitment, pornography, and dangerous content.
- Provides a roadmap for White Supremacists and fraudsters to circumvent protections
- Makes it more difficult for service providers to block SPAM.
- Florida tried this and was ruled unconstitutional, and South Carolina rejected it

AB 587 discourages the moderation of content we don't want on our platforms and will result in many of the problems we outline below.

AB 587 impedes the ability of websites and platforms to remove terrorist recruitment, pornography, and dangerous content

Today, online websites and platforms take significant steps to remove terrorist recruitment, pornography, and dangerous content from their sites. In just the six-months from July to December 2018, Facebook, Google, and Twitter took action on over 5 billion accounts and posts.¹ This includes the removal of 57 million instances of pornography. 17 million instances of content related to child safety.

Yet the removal of content related to extremist recruitment, pornography, and child safety is impeded by AB 587. This is because it forces platforms to set explicit criteria they will use in determining whether to disable or suspend a user's social media website account and to notify users with an explanation of why their account was taken down in the case of a removal. This locks social media platforms into a specific content moderation regime and greatly limits their ability to respond quickly and effectively in the face of emerging circumstances.

Imagine an white-nationalist group making posts that simply read, "Join us to help Clean-up America." Blocking or removing their account would be more difficult under AB 587, as platforms likely would not have criteria that specifically prohibit this type of content.

There are also things like the "Tide Pod Challenge" and the "Salt and Ice Challenge" that may not clearly violate any specific standard set by the platforms, but still need to be moderated as they put the safety of children at considerable risk. The provisions in this bill would make it harder for platforms to respond

¹ See Transparency Report, at http://netchoice.org/wp-content/uploads/Transparency-Report.pdf

rapidly as these dangerous and objectionable movements emerge. It also makes it more difficult to stop child predators as shown in the attached declaration of the similar Florida law.

The end result is that websites and platforms will err on the side of leaving up lewd, lascivious, dangerous, and extremist speech and content, making the internet a much more objectionable place to be. Further, users are already protected from unfair trade practices and the government can currently bring suits against the platforms if they truly believe these companies are engaging in unfair practices.

Provides a roadmap for White Supremacists and fraudsters to circumvent protections

Platforms often don't tell bad actors which words, phrases, or content result in removal. This is because with such information the bad actors can circumvent the system. Consider a prohibition on profanity. Bad actors could simply add an "*" to beat the blockers.

Likewise consider a ban on swastikas. Bad actors could slightly modify the images to avoid removal. In the end, AB 587 will make it easier for bad actors and horrible content to exist on platforms by giving them the secrets to avoid removal.

AB 587 makes it difficult for providers to block SPAM

Today, platforms engage in robust content blocking of SPAM. But this blocking of not only unwanted but invasive content would be far more difficult under AB 587, as it would need to violate some explicit criteria previously set by the specific platform at issue.

For decades, service providers have fought bad actors to keep our services usable. Through blocking of IP and email addresses along with removing content with harmful keywords, our services are more useful and user friendly. But services couldn't do this type of blocking under AB 587 unless they had specific criteria that cover the content in question.² Defenders of the bill may argue that platforms could still adopt a standard that broadly prohibits SPAM, but then each case of removal would subject the platforms to legal action based on the specific facts and content at issue. SPAM is not uniform in nature and can be difficult to clearly define. As such, platforms would likely err on the side of leaving up more SPAM than they would otherwise.

Diminishing platform's ability to remove SPAM content would contradict Congress's intent to "remove disincentives for the development and utilization of blocking and filtering technologies."³

Florida tried this and was ruled unconstitutional, and South Carolina rejected it

Earlier this year, Florida Governor DeSantis enacted similar legislation that to prevent platforms from removing bad actors and disinformation. The Florida law, in part, required, "A social

² See, e.g. Holomaxx Technologies Corp. v. Microsoft, 783 F. Supp. 2d 1097 (N.D. Cal. 2011) (That case involved an email marketer sued Microsoft, claiming that the SPAM blocking filtering technology Microsoft employed was tortious.)

³ *Id.* at 1105 (citing 47 U.S.C. § 230(b)(4)).

media platform must publish the standards, including detailed definitions, it uses or has used for determining how to censor, deplatform, and shadow ban."⁴

The Florida law's requirements for publication mirror the requirements of AB 587 – although for diametrically opposite political purposes. Nonetheless, a Federal Court found that compelled speech mandates, like the ones seen in AB 587, are a patently unconstitutional violation of the First Amendment.⁵

Because it restricts the ability of social media websites to moderate objectionable content and block SPAM, we respectfully ask you to **oppose AB 587**.

We appreciate your consideration of our views, and please let us know if we can provide further information.

Sincerely,

Carl Szabo

Vice President and General Counsel, NetChoice NetChoice works to make the Internet safe for free enterprise and free expression. www.netchoice.org

⁴ Florida SB 7072 (2021).

⁵ See, NetChoice, LLC v. Moody, 2021 WL 2690876 (N.D. Fla. June 30, 2021)

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF FLORIDA TALLAHASSEE DIVISION

NETCHOICE, LLC d/b/a NETCHOICE, a District of Columbia organization; and COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION d/b/a CCIA, a Virginia corporation,

Plaintiffs,

v.

ASHLEY BROOKE MOODY, in her official capacity as Attorney General of the State of Florida; JONI ALEXIS POITIER, in her official capacity as Commissioner of the Florida Elections Commission; JASON TODD ALLEN, in his official capacity as Commissioner of the Florida Elections Commission; JOHN MARTIN HAYES, in his official capacity as Commissioner of the Florida **Elections Commission; KYMBERLEE** CURRY SMITH, in her official capacity as Commissioner of the Florida Elections Commission; BARBRA STERN, in her official capacity as Commissioner of the Florida Elections Commission; and PATRICK GILLESPIE, in his official capacity as Deputy Secretary of Business Operations of the Florida Department of Management Services,

Defendants.

Civil Action No.: 4:21-cv-00220-RH-MAF

DECLARATION OF STOP CHILD PREDATORS IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

I, Stacie D. Rumenap, declare as follows:

1. I am President at Stop Child Predators (SCP), an organization founded in 2005, to combat the sexual exploitation of children and protect the rights of crime victims nationwide. I have led SCP since 2006, having worked in all 50 states – including spearheading the passage in 46 states of Jessica's Law, which originated in Florida – on laws and educational efforts to bring together a team of policy experts, law enforcement officers, community leaders, and parents to launch state and federal campaigns to inform lawmakers and the public about policy changes that will protect America's children from sexual predators both online and in the real world.

2. We work with parents, lawmakers, and technology companies to better educate families, schools, and lawmakers about the potential risks children face online, including grooming, luring, bullying, child pornography, and other harms to children.

3. We also launched the Stop Internet Predators (SIP) initiative in 2008 because sex offender management and child safety must be addressed both in the real world and online. SIP recognizes that child predators often use online socialnetworking platforms to recruit child sex-trafficking victims, to groom children for sexual exploitation, and to sexually victimize children in general. Because previously convicted and registered sex offenders are the most identifiable and likely class of predators to target children online, we focus our policy efforts on keeping social media and the Internet more broadly safe for children.

4. To do this, we work with leading online platforms, including Plaintiffs' members, to develop and enforce content-moderation and safety policies that prioritize children's safety while still promoting free speech. Our goal is to help these businesses develop tools and mechanisms to identify illegal content—Child Sexual Abuse Material—as soon as possible so that children are not exposed to abuse.

5. Unfortunately, CSAM is prolific on the Internet. In 2018 alone, leading social media platforms reported over 45 million photos and videos of children being sexually abused.¹ In fact, there are so many reports of child exploitation that FBI and Department of Justice officials said it would require assigning cases to every FBI agent. The government does not presently have the resources to do that.²

6. The government's limited resources underscore the critical importance of private moderation and filtering technologies. In order to detect CSAM, as well as to report it to authorities, online companies must develop and use advanced

¹ Katie Benner & Mike Isaac, *Child-Welfare Activists Attack Facebook Over Encryption Plans*, N.Y. Times (Feb. 5, 2020), <u>https://www.nytimes.com/2020/02/05/technology/facebook-encryption-child-exploitation.html</u>. ² Id.

algorithms and other screening tools.

7. If Florida's S.B. 7072, 2021 Leg. (Fla. 2021) (the "Act") is allowed to go into effect on July 1, 2021, we are concerned that it would be harder to remove objectionable content online.

8. The online platforms we work with remove millions of pieces of content that would enable child predation and harm children. We have grave concerns that the Act will impede their ability to remove such content and undermine my group's efforts to stop child predation. Not only does the Act require online platforms to host content—legal or not—from "journalistic enterprises," it also prohibits them from using algorithms in ways that could flag, remove, restrict, or demote harmful content, including CSAM.

9. Equally concerning is the Act's limit on the number of changes online platforms can make to their algorithms each month. Under the Act, platforms may not change their algorithms more than once every 30 days. This restriction all but guarantees that the online platforms will be hamstringed in responding to new threats to children's online safety and to new methods of distributing or soliciting photos and videos of child sexual abuse. It will also hinder their ability to adapt to predators' schemes. As history and experience have shown, predators continue to find a way around existing safeguards, requiring us, the platforms, and the public to remain ever vigilant.

3

10. Similarly, the Act's disclosure requirements give child predators a roadmap to escape detection. If they know how algorithms and content moderation work in detail, they will have an even easier time preying on vulnerable children.

11. Likewise, the Act's onerous obligations for account and content removal will likely cause online platforms to moderate less aggressively. That is particularly concerning at a time when we need even more moderation and even more filtering.

12. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 2nd day of June, 2021 at 3:00 pm.

Secure Burners

Stacie D. Rumenap