AMBIKA KUMAR (*pro hac vice*)
ambikakumar@dwt.com
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue, Suite 3300
Seattle, Washington 98104
Telephone: (206) 757-8030

ADAM S. SIEFF (CA Bar No. 302030)
adamsieff@dwt.com
DAVIS WRIGHT TREMAINE LLP
865 South Figueroa Street, 24th Floor
Los Angeles, California 90017-2566
Telephone: (213) 633-6800

ROBERT CORN-REVERE (*pro hac vice*)
bobcornrevere@dwt.com
DAVID M. GOSSETT (*pro hac vice*)
davidgossett@dwt.com
MEENAKSHI KRISHNAN (*pro hac vice*)
meenakshikrishnan@dwt.com
DAVIS WRIGHT TREMAINE LLP
1301 K Street NW, Suite 500 East
Washington, D.C. 20005
Telephone: (202) 973-4200

Attorneys for Plaintiff
NETCHOICE, LLC d/b/a NetChoice

IN THE UNITED STATES DISTRICT COURT

THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

NETCHOICE, LLC d/b/a NetChoice,

Plaintiff,

v.

ROB BONTA, ATTORNEY GENERAL OF THE STATE OF CALIFORNIA, in his official capacity,

Defendant.

Case No. 5:22-cv-08861-BLF

DECLARATION OF STACIE D. RUMENAP IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

Date: June 22, 2023
Time: 9:00 a.m.
Dept.: Courtroom 3 – 5th Floor

Action Filed: December 14, 2022

I, Stacie D. Rumenap, declare:

1. ***Identity of Declarant***. I am the President of Stop Child Predators (SCP), a 501(c)(3) nonprofit 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 of Jessica's Law in 46 states. SCP brings together 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. I make this declaration from personal knowledge.

2. ***SCP's Mission***. SCP works with parents, lawmakers, and policy experts to better educate families, schools, and lawmakers about the potential risks children face both in the real world and online, including grooming, luring, bullying, child pornography, and other harms to children. SCP has worked for nearly two decades to open lines of dialogue with lawmakers and technology company stakeholders, to help them determine the best and most practical ways to protect children from these risks.

3. SCP focuses significant policy efforts on keeping social media, and the internet more broadly, safe for children. In 2008, we launched the Stop Internet Predators (SIP) initiative in recognition that child predators often use social-networking platforms to recruit child sex-trafficking victims, to groom children for sexual exploitation, and to sexually victimize children in general, and sex offender management, and that child safety must therefore be addressed both in the real world and online. Our more recent Digital Safety Project adapts the SIP initiative's goals to a new online landscape, and operates from the premise that the private sector plays an important role in protecting children. Through this project, we also work to ensure that the government doesn't unnecessarily interfere with the protection of children or the ability of parents to decide what's best for their children.

4. We believe that the internet and social media have incalculable value for our young people—particularly those who are disabled, suffer from anxiety, or are in other circumstances that make it difficult for them to connect in person. We therefore work with leading online

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
ANGELES, CALIFORNIA 90017-2566

platforms, including Plaintiff's members, to develop and enforce policies that prioritize children's safety while still promoting free speech and ensuring children have access to valuable technology. Our goal is to help businesses develop tools and mechanisms to identify and promptly take down illegal content (Child Sexual Abuse Material, or CSAM), and to help them identify products and services that may be used by predators to target and lure children. These tools and mechanisms help businesses mitigate the potential for their products and services to be used to cause harm.

5. We believe the private sector plays a critical role in limiting the proliferation of harmful content online. For example, 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. In fact, there are so many reports of child exploitation that FBI and Department of Justice officials said that investigating them would require assigning cases to every FBI agent. The government does not presently have the resources to do that. The government's limited resources underscore the importance of private moderation and filtering technologies. In order to detect CSAM, as well as to report it to authorities, online companies can (and must) develop and use advanced algorithms and other screening tools.

6. ***AB 2273***. We are concerned that AB 2273, while ostensibly intended to make the internet safer for children, will instead result in serious negative outcomes for children. For example, the law requires businesses to "[e]nforce published terms, policies, and community standards established by the business," and subjects businesses to civil liability if they do not do so adequately. We are concerned that many businesses will stop having community standards at all rather than expose themselves to liability for failing to enforce in a manner acceptable to California's Attorney General. Community standards are essential to transparent and efficient moderation of CSAM and other content that may expose children to harm, and we oppose any legislation that would discourage the establishment of community standards.

7. We are also concerned about AB 2273's requirement that covered businesses "[e]stimate the age of child users with a reasonable level of certainty." This would require businesses to collect personal information from each of their minor users, creating a trove of sensitive data regarding these children. We consider it not a risk but an inevitability, given the

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
ANGELES, CALIFORNIA 90017-2566

realities of data security, that one or more of these data sets will be breached, exposing the personal information of children to bad actors. In fact, it would be entirely consistent with predators' *modus operandi* to seek out such information, even by taking a job where they could have access to it.

8. In my work to make the internet safer for children, I have become familiar with the types of technology that companies have considered to verify the ages of their users. I understand that this technology raises accessibility concerns. For instance, a technology that requires a user to take a photograph of their own face would not be accessible to a person who does not have an integrated camera on their device, and may prove practically inaccessible to someone who is vision impaired and cannot easily take a photograph. While we believe the government should be involved in keeping the internet safe for children, we are opposed to a solution that would render portions of the internet inaccessible to disabled and under-resourced individuals.

9. AB 2273 also prohibits a covered business from "[c]ollect[ing], … shar[ing], or retain[ing] any personal information" about children or "us[ing]" children's personal information "for any reason other than a reason for which [it] was collected," unless the business can "demonstrate a compelling reason" that such activities are "in the best interests of children." The problem with these provisions is that they require tracking of children to be justified *before* it happens, when the importance of preserving this information may only emerge *after*.

10. For example, consider a child unknowingly involved in an online exchange with an older predator, who is masquerading as a young person and attempting to lure the child into a dangerous situation. If the child is ultimately entrapped, their online activity (including their conversations with the predator and their search history) could be critically helpful in finding the child, but if sites are prevented from collecting this information in the first place, this valuable evidence will be lost. In fact, a child's online activity could reveal patterns that could help private companies alert the children and their parents to something amiss, but those patterns will not come to light if they are erased before they can be analyzed. To provide an example: A child searching for information about bus routes may not be a concern on its own, but a child searching for information about bus routes immediately *after* interacting online with an adult in another state could trigger an alert to the child and/or their parents. AB 2273 strongly discourages—if not

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
ANGELES, CALIFORNIA 90017-2566

prohibits altogether—companies from using this kind of harm-prevention technology.

11. Finally, AB 2273 in a number of cases requires companies to evaluate whether content or services could be "harmful" or risk "material detriment" to children, extremely vague standards that would be subject to interpretation by each California Attorney General. By doing this, AB 2273 displaces the individual judgments of families as to what is appropriate for *their* children with the State's monolithic determination of what is appropriate for *all* children. We consider this an unnecessary interference into decisions that should be left in the hands of families. In fact, we believe that children are safer when their families, not the government, are empowered with the tools to guide and guard their online activities.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed at Washington, D.C., this 14th day of February, 2023.

Stacie D. Rumenap

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
ANGELES, CALIFORNIA 90017-2566