23-2969

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

NetChoice, LLC,

Plaintiff and Appellee,

v.

Rob Bonta, in his official capacity as Attorney General of the State of California,

Defendant and Appellant.

On Appeal from the United States District Court
for the Northern District of California

No. 5:22-cv-08861-BLF
The Honorable Beth Labson Freeman, Judge

DEFENDANT'S REPLY BRIEF

ROB BONTA
Attorney General of California
THOMAS S. PATTERSON
Senior Assistant Attorney General
ANYA BINSACCA
Supervising Deputy Attorney General
KRISTIN A. LISKA
Deputy Attorney General
State Bar No. 315994
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3916
Fax: (415) 703-5480
Email: Kristin.Liska@doj.ca.gov
Attorneys for Defendant Attorney General Rob Bonta

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

TABLE OF AUTHORITIES
(continued)

Page

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

INTRODUCTION

Online companies routinely collect, utilize, and share huge amounts of personal information from child users, often without the user's awareness. This includes deeply personal data like geolocation data or medical information. Companies' data use, such as in algorithms to maximize time spent online or selling it to third parties, are associated with several harms, including addiction-like dependency on online content, sleep loss, mental health problems, reduced educational attainment, and exposure to predators.

Concerned about such harms to children, the California Legislature passed the California Age-Appropriate Design Code. The Act's various provisions regulate companies' data and privacy practices. They are regulations of conduct, not speech, and thus do not implicate heightened First Amendment scrutiny. At most, the challenged provisions are content-neutral regulations subject to intermediate scrutiny—a standard they satisfy.

Plaintiff's contrary arguments begin from a misreading of the Act, portraying it as a censorship scheme designed to block undesirable content from children. But this misunderstanding of the Act is deeply flawed. The Act's plain language regulates a company's conduct—i.e., what information a company may collect about a child (e.g., the child's location), how it may use that data (e.g., selling it to third parties), and the default privacy settings

for users (e.g., who can see what a child posts by default). It does not dictate what speech may, must, or cannot be shown to users, nor does it block any speech from users. And it does not empower the government to remove, screen, or block speech to uses, or to force a company to do so.

When the Act is evaluated in light of its plain language and operation, none of plaintiff's arguments are persuasive. The fact that online companies publish speech does not insulate them from regulations that govern the collection, use, and sale of user data, especially that of vulnerable children. The district court's order granting a preliminary injunction should be reversed and vacated.

ARGUMENT

I. PLAINTIFFS ARE NOT LIKELY TO SUCCEED ON THEIR FIRST AMENDMENT CLAIM

As explained in the Attorney General's opening brief, the lower court erred in concluding that plaintiff was likely to succeed on its First Amendment challenge to the Act. Plaintiff's arguments to the contrary are unpersuasive.

A. The Act Regulates Conduct, Not Speech

Plaintiff and its amici claim that the Act is about censorship and that the Act regulates the speech online companies show to minors. *E.g.*, NetChoice's Response Brief ("RB") 1-2. This is so, they contend, because the Act (directly or as an intended consequence) blocks child users' access to undesirable speech on their sites. *E.g.*, RB 22. In making this argument, plaintiff fails to distinguish distinct provisions of the Act and ignores the statute's plain language.

But proper statutory analysis "begins with the statutory text" itself. *Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 951 (9th Cir. 2009) (citation omitted). Thus, an analysis of the Act's constitutionality starts with the text and operation of the distinct sections of the Act plaintiff challenges. These sections impose regulations on conduct, not speech.

1. The Act's regulations of data and privacy practices do not regulate speech

First, several sections of the Act regulate companies' data and privacy practices. These include the Act's requirement to configure default privacy settings for child users to the strictest level, Cal. Civ. Code § 1798.99.31(a)(6); to provide "prominent, accessible, and responsive tools" for children to exercise their privacy rights and report concerns, *id.*

§ 1798.99.31(a)(10); and to provide privacy information and terms of service in clear language suited to the age of likely child users, *id.* § 1798.99.31(a)(7). It also includes prohibitions on collecting personal information from child users, *id.* § 1798.99.31(b)(3), (b)(5), (b)(6); profiling child users, *id.* § 1798.99.31(b)(2)[1]; and selling, sharing, retaining, or using personal information of child users, *id.* § 1798.99.31(b)(1), (b)(3), (b)(4).

The activities covered by these regulations are *conduct*, not speech. A company's selection of default privacy settings—that is, the default settings for who can see a user's information, posts, or other activities, which a user is free to change, *e.g.*, 7-ER-4—is not speech. Nor is a company's harvesting of user data or profiling of a user. Nor are a company's uses of personal information, such as using data in algorithms to maximize a user's time online or likelihood of purchasing an advertised product. *See* 3-ER-409, 3-ER-410. And of course, selling a trove of customers' personal information to the highest bidder is quintessential economic activity, not speech.

[1] "Profiling" is defined as "any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person," such as their health or location. Cal. Civ. Code § 1798.99.30(b)(6).

Plaintiff presents two main arguments to the contrary, but neither is persuasive. First, plaintiff claims that the regulations on collecting or using data trigger First Amendment scrutiny. *See* RB 34. But the cases plaintiff points to in support are not nearly so categorical. *See id.* (citing *Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011) and *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1992)). Indeed, the Supreme Court in *Sorrell* expressly declined to address whether the collection of information was speech. *See* 564 U.S. at 570. And the Court acknowledged that a more comprehensive regulation of data and privacy, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), would have presented "quite a different case" from the law at issue there. *Id.* at 573. Rather, *Sorrell* reflects the general principle that a law that singles out a specific message or viewpoint for less favorable treatment is a content-based law subject to strict scrutiny. *See, e.g.*, 564 U.S. at 567 (statute was "directed at certain content and aimed at certain speakers").

The Act is not such a statute. It is not a content-based restriction. *See infra* at 12-14. Nor does it single out a specific message or viewpoint for less favorable treatment; rather, the Act's regulations on data and privacy practices apply to *all* companies subject to the Act regardless of the expressive message or viewpoint of any speech hosted by or from a

company. The Act is a comprehensive regulation of data and privacy akin to HIPAA, not like the laws struck down in *Sorrell* and *U.S. West*.

Second, plaintiff argues that the restrictions on the use of data will lead to censorship of speech online. *See* RB 22-23. Not so. The Act's plain language imposes restrictions on using, collecting, and selling personal information. This nowhere controls a company's speech. That a company cannot collect or sell a child's birthdate or school class list does not limit what a company can say to a child online or what speech it can give a child access to. Plaintiff points to no message that it cannot say or host because of the Act's regulation of its data use and privacy practices.

To be sure, some of the Act's regulations of data and privacy practices might have some *incidental impact* on speech. For instance, some companies do use personal information as an input in the algorithm to select what video or post to show a user. 3-ER-409, 3-ER-410. But that a law has some incidental effect on speech is not sufficient to trigger heightened First Amendment scrutiny. After all, every law "imposes some conceivable burden on First Amendment protected activities." *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 706 (1986). Thus, a law regulating conduct can have some "plainly incidental" effects on speech without triggering First Amendment scrutiny. *Rumsfeld v. Fed'n for Acad. & Inst'l Rts., Inc.*, 547

U.S. 47, 62 (2006). That a prohibition on discrimination in hiring may require an employer "to take down a sign reading 'White Applicants Only' hardly means that the law should be analyzed as one regulating the employer's speech rather than conduct." *Id.*; *see also Sorrell*, 564 U.S. at 567 (listing other examples).

So, too, here. That a company cannot use a minor's engagement data in an algorithm to automate content does not turn a conduct regulation into a speech one. After all, that restriction on personal information use does not *censor speech*. A minor is free to seek out any speech that they wish—as are all users. And companies are free to decide what speech they show to users, minor or adult. That is regulation of conduct, not speech.[2]

---

[2] Amici ACLU and ACLU of Northern California argue that the Act's prohibition on the use of "personal information of any child," Cal. Civ. Code, § 1798.99.31(b)(1), is a regulation of speech since it will restrict the use of *any* information about *any* child. *See* ACLU Amicus Br. at 19-20. This argument proceeds from a misreading of the statute. Read in context, the reference to "personal information of any child" means only personal information *collected from a user*, not *any* data about a child. *See King v. Burwell*, 576 U.S. 473, 486 (2015) (statute's words must be read "in their context and with a view to their place in the overall statutory scheme" (citation omitted)).

Moreover, "personal information" is expressly defined to exclude "publicly available information or lawfully obtained, truthful information that is a matter of public concern." Cal. Civ. Code § 1798.140(v)(2). Thus, many of the examples that amici cite would not involve use of "personal information."

2. The Act's Data Protection Impact Assessment and mitigation plan requirement do not regulate speech

Second, the Act has sections requiring an internal risk self-assessment process of data management policies. The first part of this process requires companies to prepare a Data Protection Impact Assessment (DPIA). In the DPIA, a company must identify "the purpose of the online service, product or feature, how it uses children's personal information, and the risks of material detriment to children that arise from the data management practices of the business." Cal. Civ. Code § 1798.99.31(a)(1)(B). The second half of this requirement follows the DPIA preparation, after which a company must "[d]ocument any risk of material detriment to children that arises from the data management practices of the business" and "create a timed plan to mitigate or eliminate the risk" before offering new services. *Id.* § 1798.99.31(a)(2).

Both of these aspects of the Act are regulations of a company's conduct—i.e., how it collects, maintains, and uses data—not its speech. Looking at how the DPIA requirement would operate in practice illustrates this. For instance, a company might use personal data in an algorithm that selects what posts or video a user sees to maximize the time that a user spends online. *See* 3-ER-409, 3-ER-410, 4-ER-695. In its DPIA, the

company might note that this use of data poses a risk of harm to child users, since overusing online services can lead to addiction-like behavior, lack of sleep, or poor mental health. *See, e.g.*, 4-ER-695; *see also* American Academy of Pediatrics et al. Amicus Br. at 12-13; Center for Humane Technology Amicus Br. at 12.

Alternatively, a company might utilize a minor user's personal information to connect them to other users, such as by recommending other users to message, join a group with, or "friend." But this places a minor at risk of being connected to an adult user intending to abuse or exploit the minor. 4-ER-698; *see also* American Academy of Pediatrics et al. Amicus Br. at 19; Center for Humane Technology Amicus Br. at 11. In both of these examples, the risks being identified do not stem from any *speech* from or hosted by a company, but from the company's *actions* with respect to how it uses data.

This is particularly true with respect to the mitigation plan requirement. It is true that the Act requires the DPIA to address "whether the design of the online product, service, or feature could harm children, including by exposing children to harmful, or potentially harmful, content on the online product service or feature." Cal. Civ. Code § 1798.99.31(a)(1)(B)(i). But the mitigation requirement contains *no* reference to content whatsoever; it

solely requires a company to mitigate risks from its *data management practices*. *See id.* § 1798.99.31(a)(2). Thus, even if a company might identify a risk stemming from potentially harmful content to minors in its DPIA, it is not obligated to censor or remove such content as part of a mitigation plan. It only must change its data management practices.

Plaintiff makes a similar argument (RB 21) about the Act's requirement that a company enforce its own "published terms, policies, and community standards." Cal. Civ. Code § 1798.99.31(a)(9). Again, though, this is not a direct regulation of speech. Indeed, plaintiff acknowledges that the enforcement-of-terms provision does not "expressly" censor any content (RB 21); it suggests instead that companies will feel pressured to enforce their own rules "to the State's satisfaction" (*id.*). But that concern is not tethered to the Act's plain language, which in no way limits a company's ability to set, modify, apply, or interpret its own content moderation policies. Rather, the Act simply requires a company to adhere to the agreement it has voluntarily made with its users—its terms of use, including any content moderation or community standards policies—just as companies typically must do, even when those agreements involve voluntarily imposed limitations on speech. The First Amendment does not forbid laws simply

"requir[ing] those making promises to keep them." *Cohen v. Cowles Media Co.*, 501 U.S. 663, 671 (1991).

3. The Act's age estimation requirement does not regulate companies' speech or block users' access to speech

Third, the Act requires companies to estimate users' ages to a reasonable degree of certainty. Cal. Civil Code § 1798.99.31(a)(5). To be clear, this is *not* an age verification requirement; companies do not need to have definitive proof of any particular user's age at any time, including before the user can access any speech online. Rather, a company need only estimate—that is, guess or predict—the user's age with some level of certainty. This is a regulation of conduct by requiring a company to take a certain non-speech action.

Plaintiff and its amici argue that this is a regulation of speech because it will block users' access to speech online. *E.g.*, RB 22-23. Not so. The age estimation requirement is used for purposes of determining what privacy and data collection practices apply to the user. *See* Cal. Civil Code § 1798.99.31(a)(5) (requiring companies to estimate age or apply privacy and data protections for children to all consumers). It does not require a company to limit access to any speech based on the user's age, only to modify their practices around collecting and using data and default privacy

settings. *See supra* at 3-8. Any person of any age remains just as free under the Act to sign up for or create an account and to access any speech on that service as otherwise. This is true even if a company does not estimate a user's age, since the referenced privacy and data protections do not limit a user's speech or access to others' speech online, *see supra* at 3-8. Whether age is estimated or not, any user is just as free to search for, view, post, or access any speech or expressive content under the Act as otherwise.

B. The Act Does Not Violate the First Amendment

Even if the Act is subject to First Amendment scrutiny, plaintiff has not shown a likelihood of success on its First Amendment claim.

1. The Act is not subject to strict scrutiny

Plaintiff contends that strict scrutiny, not intermediate scrutiny, is the proper standard to apply here. Its arguments as to why are unpersuasive. First, plaintiff argues that the Act's challenged sections are content-based restrictions. RB 39-41. But a law is content-based when "the underlying purpose of the regulation is to suppress particular ideas or if the regulation, by its very terms, singles out particular content for differential treatment." *Berger v. City of Seattle*, 569 F.3d 1029, 1051 (9th Cir. 2009) (en banc). The Act's purpose is not suppression of ideas; the statute itself lays out its

purposes, none of which are about suppressing speech. 7-ER-1261, *see also* Attorney General's Opening Brief ("OB"), 41.

Nor do the Act's challenged provisions single out particular messages for differential treatment. Rather, determining whether a company is subject to the Act's requirements involves looking only at neutral, *non-content* criteria: whether the service is likely to be accessed by children and the size of the company. *See* Cal. Civil Code § 1798.140(d). And all companies subject to the Act must comply with its regulations regardless of what message they wish to host or express.

Plaintiff further contends that the Act is content-based because the DPIA requires companies to consider certain topics in their report. RB 40. But companies are routinely required to report on specific information to the government, including by formulating risk assessments. *See, e.g.*, Fairplay et al. Amicus Br. at 9-18 (listing examples of other reporting requirements). Plaintiff points to no case law suggesting that a reporting requirement is content-based simply because it requires reporting on certain topics. Were that so, myriad other state and federal reporting requirements would also be content-based regulations subject to strict scrutiny. Rather, what is relevant is whether a company's obligation to report certain information is triggered by the content of a company's speech. That is not the case with the Act.

Finally, plaintiff contends that the Act is content-based because it exempts "entire categories of speakers, including government and non-profit entities." RB 40. But the Supreme Court has stated that laws that draw distinctions based on speaker identity are not automatically subject to strict scrutiny; rather, such laws "demand strict scrutiny when the legislature's speaker preference reflects a content preference." *Barr v. Am. Ass'n of Pol. Consultants*, 140 S. Ct. 2335, 2347 (2020) (citation omitted) That is not the case here, where the factors that determine a company's need to comply with the Act reflect an assessment of which companies pose the risks the Act seeks to mitigate, not any content preferences. *See* Cal. Civ. Code § 1798.140(d). Because the Act draws no distinction in the scope of regulated entities or their regulated conduct based on a company's message, it is a content-neutral law not subject to strict scrutiny

2. The Act is constitutional under the *Central Hudson* standard

As explained in the Attorney General's opening brief, the Act's challenged sections meet the four-part test for constitutional regulations of commercial speech set forth in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557 (1980). OB 40-49. In applying this test, the lower court erred by substituting its judgment on

how to balance conflicting interests. OB 46. It also demanded a stringent fit much more akin to a least restrictive means requirement than *Central Hudson*'s tailoring requirement. OB 43. Plaintiff's arguments in its answering brief continue with these same errors.

First, contrary to plaintiff's cursory argument otherwise, the Act furthers a significant, if not compelling, state interest in protecting children's privacy, health, and safety. *See, e.g.*, *New York v. Ferber*, 458 U.S. 747, 756-757 (1982) ("[A] State's interest in 'safeguarding the physical and psychological well-being of a minor' is 'compelling.'" (citation omitted)); *United States v. Yazzie*, 743 F.3d 1278, 1287 (9th Cir. 2014) (same). That is in fact the Act's stated purpose, and it is unrelated to the expression of speech. *See* 7-ER-1261, OB 9, 41.

Second, as explained in the opening brief, the Act's challenged sections directly and materially advance this interest. OB 41-48. Plaintiff again argues in a conclusory fashion that the State has not met this burden and quibbles over the studies cited in the declaration from Dr. Radesky, a professor of pediatrics and researcher specializing in minors' digital media use. But in so doing, plaintiff overlooks the other record evidence showing the harm minors suffer from data collection and privacy policies as well as how the Act serves to mitigate those harms. *See* OB 41-48. That the Act

furthers the State's interest is simple logic: if companies are using children's data in ways that lead to harm, then prohibiting the collection and use of that data will mitigate those harms.

Finally, the Act's challenged provisions are properly tailored to advance the State's interests. Under this final prong of the *Central Hudson* analysis, the fit need not be "necessarily perfect, but reasonable" and the regulation must only be "in proportion to the interest served." *Bd. of Trustees of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 480 (1989). Indeed, this Court has "not insisted that there be no conceivable alternative, but only that the regulation not 'burden substantially more speech than is necessary to further the government's legitimate interest.'" *Yim v. City of Seattle*, 63 F.4th 783, 796 (9th Cir. 2023) (quoting *Fox*, 492 U.S. at 478). And this Court has noted that "[i]n general, 'almost all of the restrictions disallowed under *Central Hudson's* fourth prong have been substantially excessive, disregarding far less restrictive and more precise means.'" *Hunt v. City of Los Angeles*, 638 F.3d 703, 717 (9th Cir. 2011) (quoting *Fox*, 492 U.S. at 479). Where the government has instead "'carefully calculated the costs and benefits associated with the burden on speech'" and "struck a 'reasonable' balance between the interests of various parties," the statute is sufficiently tailored. *Yim*, 63 F.4th at 796 (citation omitted).

Plaintiff raises several arguments as to why the Act is not properly tailored, but none are persuasive. First, plaintiff contends that the Act's challenged sections regulate too much speech to advance the State's interest, impacting "virtually all online content." RB 24-25. But as with most of plaintiff's arguments, this proceeds from a fundamental mischaracterization of what the Act does; the Act does not censor or block any content from any users—child or adult. *See supra* at 3-11.

Second, plaintiff alleges the Act is not narrowly tailored because other existing laws—namely other California privacy laws and the federal Children's Online Privacy Protection Act (COPPA)—already suffice. RB 46-47. But these laws do not have the same scope of regulation as the Act. COPPA, for instance, only applies to companies that target minors rather than those likely to be accessed by minors. And the evidence in the record established that prior privacy laws have proven insufficient in protecting children's privacy. *See* 3-ER-408, 3-ER-409, 4-ER-687-689, 4-ER-706, 4-ER-711. In any event, plaintiff nowhere explains how the preferred alternatives permit more speech than the Act does, let alone substantially more. Indeed, plaintiff fails to point to *one single thing* they cannot say under the Act but could under existing privacy regulations.

Finally, plaintiff raises cursory allegations that the various challenged sections of the Act are not tailored to further the Act's goals. Many of these arguments—such as those about the Act's regulations on collecting and using minors' data, profiling minors, privacy settings, or using dark patterns—proceed once more from the erroneous contention that such sections restrict what speech can be shown to children. *See* RB 51, 53-54. But these provisions limit the *collection and use of data*, not speech. *See supra* at 3-8. Prohibiting the use of data except when necessary to provide services or in the best interests of the child clearly protects children from harmful uses of their data. So, too, does requiring stricter privacy settings—which, again, *do not dictate what speech can or cannot be shown to a minor*—help to protect the privacy of minors and avoid the harms that can flow from violating that privacy.

Plaintiff also argues that there is no evidence that requiring companies to use age-appropriate language in describing their privacy settings would mitigate harm to minors. But it is surely common sense that the vast majority of seven-year-olds would struggle to understand a dense notice of terms of use, which even lawyers can disagree over. In any event, insofar as the State needed to present evidence to support the idea that an elementary school child would struggle to understand policies written at a college level,

that evidence *was* presented below. *See* 3-ER-395, 3-ER-396, 4-ER-693, 4-ER-694. Requiring privacy policies to be written in language a child can understand enables a child to control other users' access to their personal and thereby helps protect their privacy.

The DPIA and mitigation plan regulation also furthers the Act's purposes. Requiring companies to consider the risks their data management practices pose to children and to mitigate such risks certainly advances the State's interest in protecting minors from those risks of harm. *See* OB 44-45. Plaintiff, much like the lower court, seeks to require the State to adhere to a higher standard: demonstrating that the requirement will, with certainty, result in the State's goal being achieved. But that is not the standard. It is certainly reasonable to conclude, as the Legislature did, that mitigating risks from data management practices will result in less harm to children from companies' collection and use of their data.

Finally, plaintiff argues that the Act's age estimation requirement is not properly tailored since having to estimate a user's age requires the gathering of additional data. RB 49. But it is hard to conceive of how the State could more narrowly tailor the law. The State's interest is in protecting *minors*. That of course necessitates that an internet company apply the Act's regulations on data collection and privacy practices to minor users' accounts.

Of course, the State could simply those regulations as *all* users. Yet that would simply regulate *more*, not less.

Moreover, plaintiff ignores the numerous ways that the Act seeks to mitigate any risk from collecting data to estimate age. For one, the Act prohibits using data collected to estimate age for any other purpose and requires that such data be retained no longer than necessary to estimate age. *See* Cal. Civ. Code, § 1798.99.31(b)(8). And it allows companies to estimate age in ways that do not require collecting data. *See* 3-ER-411, 3-ER-412, 4-ER-709, 4-ER-710, 4-ER-711; *see also* EPIC Amicus Br. at 19-21, Fairplay et al. Amicus Br. at 22-25. Finally, many companies already collect sufficient data to enable age estimation and thus can simply use data they already have. 3-ER-412.

Ultimately, the requirement to estimate age is an example of how the Legislature must balance competing interests when crafting a law. How to strike that balance is a policy judgment best left to the Legislature. Plaintiff's disagreement with how the Legislature chose to strike that balance here does not make the statute unconstitutional. Plaintiff has failed to establish that any overbreadth is not only "real, but substantial as well, judged in relation to the statute's plainly legitimate sweep to justify

invalidating the statute on its face." *Coyote Pub'g, Inc. v. Miller*, 598 F.3d 592, 610 (9th Cir. 2010) (citation omitted).

C. Plaintiff's Other First Amendment Arguments Are Unpersuasive

Plaintiff presents three additional arguments for why the Act violates the First Amendment. None are persuasive.

1. The Act is not a prior restraint

First, plaintiff argues (AB 19-21) that the Act is invalid because it imposes a prior restraint on speech. Not so. A regulation is a prior restraint when it "forbid[s] certain communications . . . in advance of the time that such communications are to occur." *Alexander v. United States*, 509 U.S. 544, 550 (1993) (citation omitted). The key question is thus "whether the challenged regulation *authorizes* suppression of speech in advance of its expression." *Long Beach Area Peace Network v. City of Long Beach*, 574 F.3d 1011, 1023 (9th Cir. 2009) (citation omitted) (emphasis in original). "Temporary restraining orders and permanent injunctions—*i.e.*, court orders that actually forbid speech activities—are classic examples of prior restraints." *Alexander*, 509 U.S. at 550. So, too, is a licensing or permit regime that requires permission before engaging in expressive activity. *See*,

e.g., *Long Beach Area*, 574 F.3d at 1023 (regulations requiring permit before holding demonstration in public space was prior restraint).

Even assuming that provisions of the Act could be said to regulate speech, *but see supra* at 3-11, it does not impose any *prior restraint* on speech. Only one section of the Act arguably imposes any prior conditions on operation (as opposed to sanctioning past conduct), namely the DPIA requirement. And while the requirement to prepare a DPIA is described as a precondition to offering new services, it is not a prior restraint on speech. For the Act nowhere authorizes the government to block any expressive activity if a DPIA is not prepared; nor does it require a company to submit a DPIA in order to receive permission (like a license or permit) to offer a new service. Because none of the Act's challenged sections block expressive activity, let alone before it occurs, they are not a prior restraint.

2. The Act's challenged sections are not unduly vague

Plaintiff additionally contends that the Act is unduly vague. A statute is impermissibly vague when it "fails to provide a reasonable opportunity to know what conduct is prohibited, or is so indefinite as to allow arbitrary and discriminatory enforcement." *Arce v. Douglas*, 793 F.3d 968, 988 (9th Cir. 2015) (citation omitted). But this "does not require 'impossible standards of clarity.'" *Id.* (citation omitted). Rather, the statute must simply "give a

'person of ordinary intelligence a reasonable opportunity to know what is prohibited.'" *Valle del Sol, Inc. v. Whiting*, 732 F.3d 1006, 1019 (9th Cir. 2013) (citation omitted).

Plaintiff points to a variety of isolated terms in the Act that it contends are unduly vague. All these terms are sufficiently clear. For instance, plaintiff contends that the meaning of "data management practices" is unclear. *See* RB 29. But the phrase has a plain meaning: 1) "data" refers to information, 2) "management" is the process of dealing with or controlling something,[3] and 3) "practices" is the habitual way of doing something.[4] Thus, "data management practices" is the usual way that a company controls or deals with the data it collects.

The phrase "best interest of the child"—another that plaintiff singles out as unduly vague—is also clear. Although the phrase may not be a common one in business, it is ubiquitous in the legal system. It is the standard used in California to determine child custody arrangements, *see*,

---

[3] *See, e.g.*, *Management*, Cambridge Dictionary, *available at* https://dictionary.cambridge.org/us/dictionary/english/management (last accessed Mar. 13, 2024) (defining "management" as "the control or organization of something").

[4] *See, e.g.*, *Practice*, Cambridge Dictionary, *available at* https://dictionary.cambridge.org/us/dictionary/english/practice (last accessed Mar. 13, 2024) (defining "practice" as "something that is usually or regularly done").

e.g., *In re Marriage of Vargas & Ross*, 17 Cal. App. 5th 1235, 1243 (2017); to make guardianship decisions, *see, e.g.*, *Petition of Daniels*, 177 Cal. App. 2d 376, 378 (1960); and in delinquency proceedings, *see, e.g.*, *In re Jonathan C.M.*, 91 Cal. App. 5th 1039, 1041 (2023).

The Act's reference to "dark patterns" is similarly clear. The term "dark patterns" is "widely used, acknowledged, and accepted" in the online industry. 4-ER-711. Regulatory groups have defined the term, as have those who conduct research in field. 4-ER-696, 4-ER-497, 4-ER-711. Furthermore, California law includes a definition of "dark pattern". *See* Cal. Civ. Code § 1798.140(*l*). Given the common use of the phrase in the relevant industry combined with the statutory definition, the meaning of "dark patterns" is not unconstitutionally vague.

Finally, plaintiff takes issue with some of the phrases used in the examples of content to include in the DPIA. RB 28. But the requirement to complete the DPIA and its main content—identifying the purpose of the company's product, how it uses children's personal information, and the risks to children from its data management practices—are clear. And even if certain topics in the DPIA could be ambiguous, the Act simply requires a company to complete a DPIA; the Attorney General does not review the

DPIA to determine if a company has correctly identified all risks, only that it has addressed the required topics.

Overall, the Act's regulations on a business's conduct are sufficiently clear. While there may be cases at the margin that could be debatable or hypotheticals that can be dreamed up, all that is required is that it be "clear what the [statute] as a whole prohibits." *Hill v. Colorado*, 530 U.S. 703, 733 (2000) (citation omitted). After all, "because we are '[c]ondemned to the use of words, we can never expect mathematical certainty from our language." *Id.* (citation omitted) (alterations in original). The Act clearly delineates the scope of restrictions on data collection and privacy policies, as well as its other restrictions, and thus it is not unduly vague.

3. The Act does not impermissibly compel speech

Plaintiff finally contends that the Act is unconstitutional because the DPIA requirement impermissibly compels speech. RB 31. But courts have long recognized that reporting requirements are permissible as part of a regulation of conduct. *See, e.g.*, *Hotel Emps. & Rest. Emps. Int'l Union v. Nev. Gaming Comm'n*, 984 F.2d 1507, 1518 (9th Cir. 1993). As discussed above, the Act is a regulation of conduct, not speech. *See supra* at 3-12. The DPIA is thus akin to other reporting requirements that are incidental to

conduct regulations, such as the one this Court upheld in *Nevada Gaming*. *See also supra* at 13 (listing examples of other reporting requirements).

Furthermore, the DPIA requirement does not obligate an individual to parrot the government's message or even to publicly speak at all. Companies are asked to self-assess certain risks, not to give a certain message or answer, and the DPIA is kept confidential and not publicly disclosed. The Attorney General's sole job is to ensure that the DPIA is completed, not to grade its content. The DPIA requirement thus fits within the type of reporting requirements that have been upheld against compelled speech challenges and are commonplace in the law.

II. PLAINTIFF IS NOT LIKELY TO SUCCEED ON ITS OTHER CLAIMS

Plaintiff contends that the preliminary injunction may alternatively be sustained because the Act violates the dormant Commerce Clause or is preempted by federal law. The lower court declined to address these arguments below. This Court should do so as well. *See, e.g.*, *Foti v. City of Menlo Park*, 146 F.3d 629, 638 (9th Cir. 1998). In any event, plaintiff is not likely to succeed on either of these alternative theories.

A. Dormant Commerce Clause

While the Commerce Clause is a grant of power to Congress to regulate interstate commerce, it also imposes "a self-executing limitation on the

power of States to enact laws imposing substantial burdens" on interstate commerce. *Ass'n des Eleveurs de Canards et d'Oies du Quebec v. Harris*, 729 F.3d 937, 947 (9th Cir. 2013) (citation omitted). This "dormant" Commerce Clause "prohibits the enforcement of state laws 'driven by . . . economic protectionism—that is, regulatory measures designed to benefit in-state economic interests by burdening out-of-state competitors.'" *Nat'l Pork Producers Council v. Ross*, 598 U.S. 356, 369 (2023) (citation omitted).

Where a statute is not facially discriminatory, a plaintiff may be able to state a claim for a dormant Commerce Clause violation under the balancing test from *Pike v. Bruce Church, Inc.*, 397 U.S. 137 (1970). *Nat'l Pork*, 598 U.S. at 379-380. The Supreme Court most recently addressed the *Pike* framework in *National Pork*, though the five justices in the majority did not agree on a single approach "to [*Pike*] challenges premised on . . . nondiscriminatory burdens." *Nat'l Pork*, 598 U.S. at 379 (internal quotation marks omitted). The upshot of *National Pork* is that this Court's precedent on the relevant *Pike* analysis remains good law. *See generally Lopez-Marroquin v. Garland*, 9 F.4th 1067, 1073-1074 (9th Cir. 2021).

Plaintiff makes a conclusory argument that the Act imposes a substantial burden on interstate commerce because it "regulates the internet," an "instrumentality of commerce" that requires "one uniform

system, or plan of regulation." RB 55-56. But a state regulation does not impose a substantial burden on interstate commerce simply because it applies to an instrumentality of interstate commerce. *See, e.g.*, *Ward v. United Airlines, Inc.*, 986 F.3d 1234, 1242 (9th Cir. 2021) (law regulating labor conditions for airline workers did not impose a substantial burden).

Nor has plaintiff established that the Act regulates in an area that requires uniformity. "To show the threat of inconsistent regulation, Plaintiffs 'must either present evidence that conflicting, legitimate legislation is already in place or that the threat of such legislation is both actual and imminent." *Rocky Mountain Farmers Union v. Corey*, 730 F.3d 1070, 1104-1105 (9th Cir. 2013) (citation omitted). Plaintiff has not shown any such conflicting restrictions here. And since plaintiff has not established a substantial burden, this Court need not consider whether that burden is clearly excessive compared to the putative and actual benefits of the law. *Nat'l Ass'n of Optometrists & Opticians v. Harris*, 682 F.3d 1144, 1155 (9th Cir. 2012).

Nor does the Act regulate wholly extraterritorial conduct. *See* RB at 56. The Act regulates only companies that do business in California and provide an online service likely to be accessed by children residing in California. Cal. Civ. Code § 1798.99.30(b)(1), 1798.140(d), (i). Websites

are capable of determining the location of users. *See* 3-ER-412-416. Thus, the Act has no impact on transactions wholly outside the State. *See Greater L.A. Agency on Deafness, Inc. v. Cable News Network*, 742 F.3d 414, 433 (9th Cir. 2014) (rejecting argument that California law requiring closed captioning on websites did not regulate extraterritorial conduct).

B. Preemption

Plaintiff argues that the Act is preempted under a conflict preemption theory, which provides that state law is preempted when it "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress," *Jones v. Google LLC*, 73 F.4th 636, 644 (9th Cir. 2023) (citation omitted). But neither of the two laws that plaintiff identifies—COPPA or Section 230 of the Communications Decency Act—preempts the challenged provisions of the Act.

1. COPPA

Plaintiff argues in passing that the Act is preempted by COPPA, which sets privacy regulations for businesses that offer online services directed toward children under 13. *See generally* 15 U.S.C. §§ 6501–6506. This is so, it claims, because COPPA and the Act have different scopes. *See* RB 57. But that difference in scope alone does not show any conflict between the two or that the Act undermines federal policy in COPPA.

2. Section 230

Finally, plaintiff contends that the Act is preempted by Section 230 of the Communications Decency Act. Section 230 prohibits a "provider or user of an interactive computer service" from being "treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. §230(c)(1).

Plaintiff argues that the Act conflicts with Section 230 by "empower[ing] the State to limit providers' discretion to review, edit, promote, and decide whether to publish user content." RB 58. As an initial matter, the Act does no such thing. The Act solely requires that companies enforce their published terms of use; it does not empower the Attorney General to second-guess *how* companies enforce those terms of use.

Moreover, nothing in Section 230 prevents a State from holding businesses accountable for *their own conduct*. *See, e.g.*, *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 682 (9th Cir. 2019) (rejecting Section 230 immunity for processing rental bookings posted by others on website); *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1107-1109 (9th Cir. 2009) (promissory estoppel claim not preempted given company's promise to remove fake profiles). Section 230 thus does not preempt the Act.

III. THE ACT IS SEVERABLE

Plaintiff challenges distinct requirements of the Act on various grounds. This Court should consider each section individually, rather than applying each argument to the Act wholesale. *See, e.g.*, *Long Beach Area*, 574 F.3d at 1044 (concluding some parts of regulation constitutional and some unconstitutional). So, too, should this Court look to any specific provision that it concludes is unconstitutional—though the Attorney General disputes that any part of the Act is unconstitutional—to conduct the severability analysis. *See id.* (remanding for severability analysis as to unconstitutional provisions).[5]

Thus plaintiff errs in contending the entire Act must be enjoined simply because *some* provisions may not be severable from others. This is not the proper focus of analysis. That, for instance, they contend the "age-estimation requirements underlie most other provisions," RB 60, says nothing about whether the DPIA requirement is severable from the remainder of the Act. Nor is it relevant that the various provisions of the

[5] As an illustrative example, with respect to the Act's DPIA and mitigation plan requirements, the Court could sever and enjoin: 1) only the list of specific content to be included in the DPIA in section 1798.99.31(a)(1)(B)(i) through (viii), 2) only the mitigation plan requirement in section 1798.99.31(a)(2), or 3) all of the DPIA and mitigation plan requirements.

Act are "intertwined with" one another. RB 60. Rather, the question is whether any particular unconstitutional section is grammatically, operationally, and volitionally separable from the remainder of the Act. *See* OB 49.

Plaintiff offers no real argument to rebut the fact that excising any particular challenged portion of the Act would leave the remainder grammatically intact. *See* OB 50. Nor does it offer any real argument that the various prohibitions of the Act challenged by plaintiff would operate independent of one another. *See* OB 50. And plaintiff's arguments as to volitional separability miss the mark. Although the *presence* of a severability clause may create a presumption of severability, the *absence* of one says nothing regarding volitional separability. *See, e.g.*, *Legislature v. Eu*, 54 Cal.3d 492, 535 (1991) (finding provision severable despite absence of severability clause). More critically, the question of volitional separability is "not whether a legislative body would have preferred the whole to the part,"—since "surely it would have"—but rather whether the legislative body "would have preferred that part to nothing." *Cal. Redevelopment Ass'n v. Matosantos*, 53 Cal. 4th 231, 273 (2011). Given the Legislature's grave concerns over the harms posed by data collection and

privacy practices, it would certainly have preferred to regulate something rather than nothing to protect vulnerable children.

CONCLUSION

The district court's order should be reversed and vacated.

Dated: March 13, 2024

Respectfully submitted,

ROB BONTA
Attorney General of California
THOMAS S. PATTERSON
Senior Assistant Attorney General
ANYA BINSACCA
Supervising Deputy Attorney General

s/ Kristin Liska

KRISTIN A. LISKA
Deputy Attorney General
Attorneys for Defendant Attorney General Rob Bonta

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 23-2969

I am the attorney or self-represented party.

This brief contains 6,999 **words,** including _____ words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- (●) complies with the word limit of Cir. R. 32-1.
- ( ) is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ( ) is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ( ) is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ( ) complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - [ ] it is a joint brief submitted by separately represented parties.
  - [ ] a party or parties are filing a single brief in response to multiple briefs.
  - [ ] a party or parties are filing a single brief in response to a longer joint brief.
- ( ) complies with the length limit designated by court order dated _____.
- ( ) is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Kristin Liska **Date** March 13, 2024
*(use "*s/[typed name]*" to sign electronically-filed documents)*

CERTIFICATE OF SERVICE

Case Name: ***NetChoice, LLC v. Bonta***
Case No.: **23-2969**

I hereby certify that on March 13, 2024, I electronically filed the following document with the Clerk of the Court by using the Court's Appellate Case Management System (ACMS):

DEFENDANT'S REPLY BRIEF

I certify that all participants in the case are registered ACMS users and that service will be accomplished electronically by the Appellate Case Management System.

I declare under penalty of perjury under the laws of the State of California and the United States of America the foregoing is true and correct.

Executed on March 13, 2024, at San Francisco, California.

Vanessa Jordan	s/ Vanessa Jordan
Declarant	Signature