23-2969

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

NetChoice, LLC,

Plaintiff-Appellee,

v.

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

Defendant-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

APPELLANT'S OPENING BRIEF

ROB BONTA
Attorney General of California
THOMAS S. PATTERSON
Senior Assistant Attorney General
ANYA M. BINSACCA
Supervising Deputy Attorney General
ELIZABETH WATSON
Deputy Attorney General
State Bar No. 295221
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3847
Email: Elizabeth.Watson@doj.ca.gov
Attorneys for Defendant-Appellant

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

TABLE OF AUTHORITIES
(continued)

Page

CONSTITUTIONAL PROVISIONS

COURT RULES

OTHER AUTHORITIES

INTRODUCTION

Online platforms facilitate important speech and commerce. They also enable exploitation. Through automation, online platforms are able to collect personal data on an unprecedented scale. And they have an economic incentive to collect and exploit that data—from both adult users and also from children. The harms that this has caused to children has been extensively documented, leading many, including the U.S. Surgeon General, to express concern.[1]

Like many states, California has attempted to address these issues through legislation. The statute at issue in this case, the California Age-Appropriate Design Code Act ("the Act"), places limits on how and when businesses collect and exploit children's data. The Act does not single out businesses based on viewpoint or the content of businesses' speech. Nor does it regulate what businesses say. It is a neutral—and needed—regulation of economic activity that, through a variety of provisions, strikes a balance between the needs of businesses and those of children without impinging on anyone's speech.

The district court decision, which preliminary enjoined the Act in its entirety, reflects significant errors of law. The court mischaracterized as regulations of speech provisions that, in fact, neutrally regulate economic activity, leading the

[1] U.S. Surgeon Gen., Advisory, *Social Media and Youth Mental Health* (2023).

court to apply the wrong standard of review. The district court misapplied the Supreme Court's decision in *Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011), ignoring that the factors that led the Court to find fault with the viewpoint-targeted data use restrictions in that case simply are not present here. The district court, relying not on evidence in the record but on vague speculation from amicus briefs, dramatically overstated the effect that various provisions would have on internet speech. The district court failed to recognize the linkages between the Act's specific provisions and the reduction of the specific harms to children that California—like other States—is seeking to address. And the district court treated the Act as an indissoluble unit, in contravention of California severance principles. Left uncorrected, these mistakes could harm not only this attempt by California to address significant risks to children, but other attempts by other governments as well. The decision should be reversed.

JURISDICTIONAL STATEMENT

The district court had subject matter jurisdiction under 28 U.S.C. §1331. The district court entered its preliminary injunction September 18, 2023, 1-ER-46, and Defendant filed a timely notice of appeal on October 18, 2023. 7-ER-1271–77; *see* Fed. R. App. P. 4(a)(1)(A). This Court has jurisdiction under 28 U.S.C. §1292(a)(1).

STATUTORY AUTHORITIES

Relevant statutory and constitutional authorities appear in the Addendum to this brief.

ISSUES PRESENTED

1. Whether the district court erred in applying heightened scrutiny to provisions of the California Age-Appropriate Design Code Act that regulate businesses' collection and use of children's data?

2. Whether the district court erred in determining that Plaintiff was likely to succeed on its claim that the Act violates the First Amendment?

3. Whether the district court erred in enjoining the Act in its entirety, in violation of California severability principles?

STATEMENT OF THE CASE

A. Factual and Statutory Background

1. Data Collection and Use Practices and Their Impact on Children

California enacted the Act against a business backdrop in which online businesses have financial incentives to collect, sell, and use an astonishing array of data about their users—a backdrop explained through declarations from Serge Egelman, Ph.D., Research Director at the Usable Security and Privacy Group and research scientist in UC Berkeley's Electrical Engineering and Computer Sciences Department who has been researching online privacy for nearly twenty years, 3-

ER-389–431, and Jenny S. Radesky, M.D., tenured Associate Professor of Pediatrics and the Director of the Division of Developmental Behavioral Pediatrics at the University of Michigan Medical School and C.D. Mott Children's Hospital, who has been researching child social-emotional development and digital media for fifteen years, 4-ER-677–740.

a. Businesses' Data Collection and Use Practices

The collection, sharing, selling, and other use of personal data provides substantial revenue for online businesses. 3-ER-392. Businesses collect user data such as names, addresses, email addresses, IP addresses, commercial information, browsing history, search history, geolocation data, and information regarding a consumer's interaction with an internet website. 3-ER-393–94; Cal. Civ. Code §1798.140(v) (defining "personal information").[2] Businesses are able to link or associate data to unique individuals through persistent identifiers, like the device an individual uses to access the internet, which tend not to change over time. 3-ER-394. Once data is linked to an individual, businesses can create a thorough individual profile, which they use to learn, predict, or infer things like users' interests, preferences, and behaviors, as well as health conditions and socioeconomic status. *Id*. For example, geolocation information can allow

[2] All statutory references are to the California Civil Code unless otherwise noted.

businesses to accurately predict very personal information—for instance, about a user's health, religious affiliation, and sexual orientation—based on where the user is located when connecting to services. *Id*.

Once a business has compiled a profile, it can be used or sold to third parties to create targeted advertising and learn more about consumer behavior to maximize profit, among other things. 3-ER-392–94; 4-ER-699–701, 704. Indeed, businesses selling and sharing of data is an essential source of revenue for many online platforms. 3-ER-392; 6-ER-1166 (IMDb explaining how data collection and use generates revenue for its business); 7-ER-1191 (same for Goodreads). And children's data is a central part of this market. A recent study of just under 6,000 children's apps showed that 19% of them collected children's data without verifiable parental consent and sold or shared that data with third-parties who indicated they would use the data for purposes including behavioral advertising. 3-ER-406. Moreover, 40% transferred children's data insecurely, putting it at higher risk of getting into the wrong hands. *Id*. And the selling, sharing, and other use of children's data has far-reaching consequences. It can be used not just for manipulative marketing campaigns, but also to feed biased and unaccountable algorithms used to make decisions about the child's future or even malicious uses, like a non-custodial parent purchasing location data to geolocate a child. 3-ER-405, 409–10; 4-ER-687–89, 704.

b. Children's Vulnerability on the Internet

Children spend a large part of their day on the internet. 4-ER-683–85. Children under two average about 50 minutes of digital technology use per day. 4-ER-685. Daily use rises to over two hours by age four, five hours by age twelve, and eight hours by age 17. *Id.* During the COVID-19 pandemic, children's access to digital technology and time online increased dramatically. 4-ER-685–86. Because children use the internet for both educational and entertainment purposes, unplugging is not a realistic option. 4-ER-686.

Children have characteristics, however, that hinder their ability to protect themselves in online environments. 4-ER-691–694. Children have less impulse inhibition and ability to engage in critical thinking and abstract reasoning about complicated concepts (like data collection) than adults. 4-ER-692–694. They also have more curiosity and attraction to novelty than adults, and greater responsivity to parasocial and peer relationships and rewards than adults. 4-ER-693–93. These characteristics are developmentally adaptive and help children learn and build social relationships in non-digital spaces. 4-ER-692.

But these characteristics can be taken advantage of through digital design. *Id.* Businesses design their services to optimize revenue generation by, among other things, maximizing time spent using the product, and increasing interactions and content generation. 4-ER-694–702; 3-ER-392–93, 409–10. For example, multiple

interview studies show that children and teens feel like they spend too much time online, feel pressure to engage, and find it hard to stop using platforms. 4-ER-695–96. Internet businesses take advantage of so-called dark patterns such as heightening parasocial relationship pressure, fabricated time pressure, and navigation constraints. 4-ER-696–97; *see also* 3-ER-410–11. One study showed that these features occurred in 80% of apps played by *preschool*-aged children and were especially common in apps played by children from lower-income and lower-education households. 4-ER-696–97. Businesses design features to direct children towards activities like extreme content generation (for instance, online challenges), which provide validation, or other harmful activities, such as disordered eating, self-harm, or gambling. 4-ER-698–702. Moreover, children are in many respects are particularly ill-equipped to evaluate the benefits of privacy and the harms of sharing private information—or even to realize when their privacy is being compromised. *See* 3-ER-397–399, 405. They are not well situated, for instance, to understand what default privacy settings a business applies, how those settings operate, and how to change them. *See* 3-ER-397 (describing 2012 study documenting difficulty users had interacting with early Facebook interface).

The Act is not the first or the only attempt to address children's privacy needs in the internet context. At the federal level, the Children's Online Privacy Protection Act (COPPA) requires that online businesses protect the personal

information of children if the platform is "directed to" children under 13. 15 U.S.C. §§6501–6506. But as many have noted, COPPA's coverage formula is underinclusive. 3-ER-407–09. Except for websites that *self*-identify as targeting children as their primary audience, websites are only required to prevent the disclosure of personal information from "visitors who identify *themselves* as under age 13." 16 C.F.R. §312.2 (emphasis added).

California regulates the collection and use of consumer data by requiring businesses to notify consumers that their data is being collected and giving consumers the right to direct businesses not to sell or share that information, §1798.100; §1798.120(a), and generally prohibiting businesses from selling or sharing the personal information of a user that the business has actual knowledge is under 16. §1798.120(c). Other laws address specific aspects of children's internet use but not the collection and use of children's data. *See, e.g.*, Cal. Bus. & Prof. §22580 (addressing online promotion of products like alcohol to minors); *id.* §22581 (addressing minors' ability to have their own online posts removed by request).

2. The California Age-Appropriate Design Code Act

The statute at issue here—the California Age-Appropriate Design Code Act—was designed to fill those gaps. It is modeled after the United Kingdom's Age Appropriate Design Code, commonly referred to as the "Children's Code[,]"which

requires that all websites likely to be accessed by children provide privacy protections by default. 3-ER-437–439, 441–44; 5-ER-457–503 (copy of the Children's Code). Online businesses operating in the U.K., which include some of Plaintiff's members, were required to bring their services into compliance with the Code by September of 2021. 3-ER-440.

California's Act was motivated by the Legislature's belief that "children should be afforded protections not only by online products and services specifically directed at them but by all online products and services they are likely to access[,]" and supported by its findings that businesses "should consider the best interests of children when designing, developing and providing" services; and that "[i]f a conflict arises between commercial interests and best interests of children, companies should prioritize the privacy, safety, and well-being of children over commercial interests." §1798.99.29.

The Act applies to companies that trade in personal information. Regulated businesses either share control, branding, and consumers' personal information with or are themselves for-profit entities operating in California that collect consumers' personal information or have it collected on their behalf, determine the purposes and means of processing that information, and have an annual gross revenue of more than $25,000,000; buy, sell, or share the personal information of 100,000 or more consumers annually; or derive 50% or more of their annual

revenues from selling or sharing that information. §1798.140(d) (incorporated into the Act through §1798.99.30(a)). Certain joint ventures or partnerships are also subject to the Act. *Id*.

Within that group of businesses, the Act regulates only those that provide an online service, product, or feature (collectively "service") "likely to be accessed by children." §1798.99.31(a), (b). "Likely to be accessed by children" means that the business's offering: (1) "is directed to children as defined by [COPPA]"; (2) "is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children[,]" or is "substantially similar or the same as" a service for which such a determination has been made; (3) contains "advertisements marketed to children[;]" (4) "has design elements that are known to be of interest to children, including but not limited to, games, cartoons, music, and celebrities who appeal to children[;]" or (5) "is determined, based on internal company research," to have children as "a significant amount of" its audience. §1798.99.30(b)(4). Broadband internet access, telecommunications services, delivery and use of a physical product, and certain medical information is excluded from regulation. §1798.99.30(b)(5); §1798.99.40.

a. Data Protection Impact Assessments

The Act requires covered businesses to complete a Data Protection Impact Assessment ("DPIA") for each service or group of services likely to be accessed by

children. §1798.99.31(a)(1). A DPIA must "identify the purpose" of the service, "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." §1798.99.31(a)(1)(A)–(B). A DPIA conducted for compliance with any other similar law, such as the U.K. Children's Code, will be considered compliant with this provision of the Act. §1798.99.31(c)(1). (Although not acknowledged in Plaintiff's submissions, many of Plaintiff's members do business in the U.K. and have presumably completed U.K. Children's Code DPIAs that would suffice for their obligations under this section of the California Act. 3-ER-451–452 (NetChoice members Google, Meta, Snap, TikTok and Twitter (now known as X) have all announced changes in compliance with the Children's Code.))

A DPIA must address, to the extent applicable, whether the design of the service could (i) "harm children, including by exposing children to harmful or potentially harmful content[;]" (ii) "lead to children experiencing or being targeted by harmful or potentially harmful contacts[;]" (iii) "permit children to witness, participate in, or be subject to harmful or potentially harmful conduct[;]" or (iv) "allow children to be party to or exploited by a harmful, or potentially harmful, contact[.]" §1798.99.31(a)(1)(B)(i)–(iv).

The DPIA must also address whether algorithms and targeted advertising systems used could harm children; whether and how the service "uses system

design features to increase, sustain, or extend use of" the service ("including the automatic playing of media, rewards for time spent, and notifications"); and whether, how, and for what purpose the service "collects or processes sensitive personal information of children." §1798.99.31(a)(1)(B)(v)–(vii).

The business must "[d]ocument any risk of material detriment to children that arises from the data management practices" in the DPIA and "create a timed plan to mitigate or eliminate the risk before" the service is accessed by children. §1798.99.31(a)(2). Regulated businesses must review their DPIAs every other year. §1798.99.31(a)(1)(A).

The DPIA is an *internal* and *confidential* document. A company has no obligation to disclose its DPIAs to the public. §1798.99.31(a)(4)(B). Regulated businesses need not deliver DPIAs to the State on a routine basis, although they must provide the Attorney General with a list of their DPIAs upon written request. §§1798.99.31(a)(3). They must also provide the Attorney General with specific DPIAs that the Attorney General requests, §1798.99.31(a)(4), but such a disclosure to the Attorney General does not vitiate the document's legal privileges. §1798.99.31(a)(4)(C).

b. Required Actions

The Act also requires regulated businesses to take other actions. They must "[e]stimate the age of child users with a reasonable level of certainty appropriate to

the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers."[3] §1798.99.31(a)(5). They must also "[c]onfigure all default privacy settings provided to children" to "offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interest of children." §1798.99.31(a)(6). They must "[p]rovide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access the service[.]" §1798.99.31(a)(7). And they must "[p]rovide an obvious signal to the child when the child is being monitored or tracked" by another user. §1798.99.31(a)(8). Businesses must "[e]nforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children." §1798.99.31(a)(9). And, they must "[p]rovide prominent, accessible, and responsive tools to help children" or their guardians "exercise their privacy rights and report concerns." §1798.99.31(a)(10).

The Act also contains other protections for children's privacy. Regulated businesses cannot use any child's data "in a way that the business knows, or has

[3] Any information that businesses collect to estimate age may be used for that purpose only, and may not be retained by businesses "any longer than necessary to estimate age." §1798.99.31(b)(8). "Age assurance shall be proportionate to the risks and data practice of an online service[.]" *Id.*

reason to know, is materially detrimental to the physical health, mental health, or well-being of a child." §1798.99.31(b)(1). They cannot "collect, sell, share, or retain any personal information that is not necessary to provide" a service "with which a child is actively or knowingly engaged" absent a "compelling reason" that the practice "is in the best interest of children likely to access" the service. §1798.99.31(b)(3); but see *id.* §1798.145 (allowing information practices that are needed to comply with other laws). Businesses also cannot use personal information of a child-user "for any reason other than a reason for which [it] was collected" absent some "compelling reason" that the other use "is in the best interest of children." §1798.99.31(b)(4).

Regulated businesses are prohibited from "profil[ing] a child by default"—that is, engaging in "automated processing" of data "to evaluate certain personal aspects relating to a natural person"—unless the business has "appropriate safeguards in place to protect children" and profiling is either "necessary to provide" the requested service and limited to the aspects of the service "with which the child is actively and knowingly engaged[,]" or the business can "demonstrate a compelling reason that profiling is in the best interest of children." §1798.99.31(b)(2); §1798.140(z).

Regulated businesses cannot "collect, sell, or share any precise geolocation information of children by default unless" it "is strictly necessary" to provide the

requested service "and then only for the limited time" necessary to provide that service, and businesses cannot collect this information "without providing an obvious sign to the child for the duration of that collection[.]" §1798.99.31(b)(5)–(6).

Finally, regulated businesses cannot use "dark patterns"—"interface[s] designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice"—"to lead or encourage children to provide personal information beyond what is reasonably expected to provide" the service, "to forgo privacy protections, or to take any action that the business knows or has reason to know is materially detrimental to the child's physical health, mental health, or well-being." §1798.99.31(b)(7); §1798.140(l).

c. Enforcement & Guidance

Regulated businesses must comply with the above requirements, including completing DPIAs, by July 1, 2024. §1798.99.31(d); §1798.99.33. There is no private right of action to enforce the Act. §1798.99.35(d). The Attorney General may sue for injunctive relief. §1798.99.35(a). The Attorney General may also seek civil penalties, with intentional violations being penalized more harshly than negligent ones. §1798.99.35(a) (penalty of up to $7,500 per affected child for intentional violations and up to $2,500 per child for negligent ones). Businesses in substantial compliance with the DPIA requirement, however, are protected from

enforcement actions by a notice-and-cure provision: §1798.99.35(c). The Attorney General may not sue without first giving notice of alleged violations and providing the company with 90 days to cure the violation and take sufficient measures to prevent future ones. *Id*.

The Act allows the Attorney General to adopt regulations related to the Act. §1798.99.35(e). And it creates the California Children's Data Protection Working Group, with members to be appointed by the Governor, members of the Legislature, and the Attorney General. §1798.99.32. The Working Group must issue a publicly available report containing best practices for implementation of the Act by January 1, 2024 (six months before the Act mandates compliance) and every two years thereafter. *Id.* Regulated businesses "may look to guidance and innovation in response to" the U.K. Children's Code when developing services likely to be accessed by children. AB 2273, §1(d).

B. Procedural Background

Plaintiff NetChoice is a trade-group whose members consist of tech companies such as Google, Meta, TikTok, Snap, Inc., and X Corp. (formerly known as Twitter). 7-ER-1231 (providing link to NetChoice membership list). NetChoice sued California's Attorney General, alleging that the Act violates the First, Fourth, and Fourteenth Amendments, and the Due Process and the Dormant Commerce Clauses; that the Act is preempted by federal law; and that the Act is

void for vagueness. 7-ER-1229–57. Plaintiff moved for a preliminary injunction based on all but its Fourth Amendment claim. 5-ER-856–897.

Plaintiff submitted, among other things, more than ten articles, some of which contained highly technical concepts or were sourced from academic journals. *See, e.g.,* 6-ER-953–57, 973–89; 2-ER-233–63. But the articles were not accompanied by declarations explaining their meaning, or verifying their reliability or veracity. In fact, Plaintiff submitted no expert evidence at all.

In opposition to Plaintiff's motion, the Attorney General submitted the declarations of two expert witnesses and a U.K. Commissioner. As noted above, Jenny S. Radesky, M.D., tenured Associate Professor of Pediatrics and the Director of the Division of Developmental Behavioral Pediatrics at the University of Michigan Medical School and C.D. Mott Children's Hospital, has been researching child social-emotional development and digital media for fifteen years. 4-ER-678–83, 716–40. She explained how children interact with technology; how businesses are incentivized to monetize children's digital experiences; why children are especially vulnerable in online spaces; how online platforms designed for adults pose risks to children through, among other things, manipulative design, frictionless contacts, targeted advertising, algorithmic application of extreme content, and lack of policy enforcement; and how the Act addresses the risks associated with these factors. 4-ER-683–713. Serge Egelman, Ph.D., Research

Director at the Usable Security and Privacy Group and research scientist in UC Berkeley's Electrical Engineering and Computer Sciences Department, has been researching online privacy for nearly twenty years. 3-ER-390–92, 420–431. He explained how online platforms are designed to make it difficult for consumers to control their data, how violations of children's privacy persist despite federal law, and how the Act operates to increase protections for children's privacy. 3-ER-392–417. And Emily Keaney, Deputy Commissioner of Regulatory Policy for the U.K. Information Commissioner's Office, explained the reasons that the U.K. adopted its similar Children's Code, how the Code has been implemented in practice, and the positive impact implementation has brought in the U.K. 3-ER-343–455.

On September 18, 2023, the court issued an order enjoining the Act in its entirety. 1-ER-2–46. The court believed that the Act was subject to heightened First Amendment scrutiny because the law infringed on businesses' right to collect and use children's data, compelled speech, and infringed on the rights of third-party internet users to access information. 1-ER-11–17. And, the court continued, the Act did not survive such scrutiny because, despite substantial evidence to the

contrary, the court determined that the Act's methods were not narrowly tailored to advance a substantial state interest.[4] 1-ER-17–38.

STANDARD OF REVIEW

This Court reviews a preliminary injunction for an abuse of discretion. *California v. Azar*, 950 F.3d 1067, 1082 (9th Cir. 2020) (en banc). "But legal issues underlying the injunction are reviewed de novo because a district court would necessarily abuse its discretion if it based its ruling on an erroneous view of law." *Id.* (internal quotation marks omitted).

SUMMARY OF ARGUMENT

The district court preliminarily enjoined the California Age-Appropriate Design Code Act in its entirety. It did so on faulty reasoning.

The First Amendment allows States to regulate economic activity. Though such regulation may incidentally affect speech, heightened scrutiny applies only where the economic regulation is viewpoint discriminatory. The court made no such finding here, and none would be warranted. Instead the court believed that heightened scrutiny of laws regulating data collection and use was required under *Sorrell v. IMS Health Services*, 564 U.S. 552 (2011). But the court misunderstood that case. *Sorrell* applied heightened scrutiny to a regulation of data use that was

[4] The court did not rule on Plaintiff's Dormant Commerce Clause, preemption, vagueness, prior restraint or overbreadth claims. 1-ER-7, 38–42.

viewpoint discriminatory: the regulations singled out representatives of drug manufacturers to lessen their effectiveness in promoting certain drugs to doctors. Nothing similar can be said of the viewpoint-neutral law at issue in this case. The district court likewise erred in subjecting the Act to heightened scrutiny under a compelled speech analysis. And the district court's imposition of heightened scrutiny based on speculation that online platforms would shut down or block users was unsupported both factually and legally. Nothing in the Act requires such draconian response, and nothing in the record supports that that would be the Act's result. (The district court appeared to rely mainly on speculation from amicus briefs—a poor basis on which to enjoin state law.) And even if intermediate scrutiny should apply, the district court erred in its application of that standard. The court held California to a virtually unattainable standard of perfection in devising protections for the serious, new problems addressed by the Act; in contrast, as this Court has noted: "It is well established that a law need not deal perfectly and fully with an identified problem to survive intermediate scrutiny." *Contest Promotions, LLC v. City & County of San Francisco*, 874 F.3d 597, 604 (9th Cir. 2017).

Finally, the district court erred in enjoining the *entire* Act, which contains numerous provisions that Plaintiff did not even challenge.

ARGUMENT

I. THE ACT IS NOT SUBJECT TO HEIGHTENED SCRUTINY

A. Regulation of the Collection and Use of Children's Data Is Not Subject to Heightened Scrutiny

The district court made a fundamental error in applying heightened scrutiny to the Act. The Act regulates economic activity—businesses' collecting, selling, sharing, retaining, and otherwise using children's data. In order to ensure that the State remains able to regulate economic activity for the benefit of the public, regulations of economic activity are only subject to heightened scrutiny when they are viewpoint discriminatory. However, instead of performing the necessary analysis to determine whether heightened scrutiny was warranted here, the district court erroneously held that *Sorrell* requires courts to apply heightened scrutiny to all data collection and use regulations. But *Sorrell*, which concerned a viewpoint discriminatory law, provides no such precedent. In failing to properly evaluate whether heightened scrutiny is even warranted, the district court skipped a critical step, which resulted in a reversible error. The Act is a non-discriminatory regulation of economic activity and thus should not be subject to heightened scrutiny at all.

1. Regulations of Economic Activity Are Rarely Subject to Heightened Scrutiny

The First Amendment recognizes a distinction between restrictions on protected expression and restrictions on economic activity. *Sorrell v. IMS Health*

Inc., 564 U.S. 552, 567 (2011). "[T]he First Amendment does not prevent restrictions directed at commerce or conduct" even when those provisions "impos[e] incidental burdens on speech." *Id.*; *see also HomeAway.com v. City of Santa Monica*, 918 F.3d 676, 685 (9th Cir. 2019) (quoting *Sorrell*); *Interpipe Contracting, Inc. v. Becerra*, 898 F.3d 879, 900–01 (2018) (regulations that "target[] a legitimate area of state regulation and do[] not discriminate based on viewpoint" are not subject to heightened scrutiny). Multiple cases establish that "an entity cannot claim a First Amendment violation simply because they may be subject to ... government regulation[,]" nor must such ordinary regulations withstand any judicial scrutiny stricter than rational basis review just because they have an incidental impact on the exercise of constitutional rights. *Am. Soc'y of Journalists & Authors, Inc. v Bonta* ("*ASJA*"), 15 F.4th 954, 961 (9th Cir. 2021) (collecting cases); *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 546 (1978) ("the State does not lose its power to regulate commercial activity deemed harmful to the public whenever speech is a component of that activity"). This applies to online businesses just as it does to traditional businesses. *HomeAway.com*, 918 F.3d at 685–86 (no heightened First Amendment scrutiny for ordinance regulating online booking transactions).

When a law regulates economic activity, a court must make the "threshold" determination of whether heightened scrutiny applies. *Id.* (citing cases); *ASJA*, 15

F.4th at 960 ("before conducting th[e scrutiny] analysis, we must assess whether the law regulates speech in the first place"). That threshold determination requires an analysis of "whether conduct with a significant expressive element drew the legal remedy or the ordinance has the inevitable effect of singling out those engaged in expressive activity." *Homeaway.com*, 918 F.3d at 685 (internal quotation marks omitted)*; see also Interpipe*, 898 F.3d at 896 ("to trigger First Amendment scrutiny, a conduct-based law must (1) target a particular type of entity for differential treatment, and (2) regulate the ingredients necessary to effectuate that entity's First Amendment rights.").

As this Court recently explained in *Interpipe Contracting, Inc. v. Becerra*, three considerations provide the rationale for requiring this threshold determination before applying heightened scrutiny to regulations of economic activity. 898 F.3d at 896. "First, a law regulating conduct that merely alters incentives rather than restricts the ingredients necessary for speech does not regulate conduct that is 'inherently expressive'—a necessary trait of an impermissible conduct-based regulation*." Id.* (citing, *inter alia*, *Rumsfeld v. Forum for Acad. & Inst'l Rights, Inc.* ("*FAIR*"), 547 U.S. 47, 66 (2006)). "Second, applying the First Amendment to conduct that has only an indirect effect on speech would task the courts with unwieldy line drawing exercises: how indirectly related to speech must a conduct-based restriction be to avoid First Amendment scrutiny?" *Id.* "Third, scrapping

conduct-based laws that have only an attenuated relationship to speech would have the perverse effect of invalidating legitimate exercises of state authority to protect the general health and welfare." *Id.* Because "an entity cannot claim a First Amendment violation simply because it may be subject to government regulation[,]" *ASJA*, 15 F.4th at 961 (quotation marks and ellipses omitted), it is Plaintiff's burden to show that heightened scrutiny is warranted. *See, e.g., Interpipe,* 898 F.3d at 893 n.11.

a. Regulations Must Have More Than an Incidental Effect on Speech to Be Subject to Heightened Scrutiny

To apply the threshold inquiry correctly, courts must distinguish between what is necessary to effectuate First Amendment rights from what might have an incidental effect on speech or expression. To determine whether speech or expression is directly regulated as opposed to incidentally effected, courts must look at the "inevitable effect of the [Act] in its face." *Homeaway,* 918 F.3d at 685–86. If the effect is "to regulate nonexpressive conduct[,]"the regulation is not subject to heightened scrutiny. *Id.* at 672 (citing *Sorrell*, 564 U.S. at 565). Drawing this line avoids "the absurd result that any government action that had some conceivable speech inhibiting consequence ... would require analysis under the First Amendment." *Int'l Franchise Ass'n, Inc. v. City of Seattle*, 803 F.3d 389, 408 (9th Cir. 2015).

Online platforms are not except from this rule. In *Homeaway.com*, online home-sharing platforms challenged a city ordinance that imposed certain obligations on platforms that facilitate short-term rentals. 918 F.3d at 680. In holding that the ordinance was "plainly a housing and rental regulation" not subject to heightened scrutiny, this Court rejected plaintiffs' argument that requiring online businesses to validate transactions before completing them resulted in an unconstitutional chill on businesses' speech. *Id.* at 685–86. Such "incidental burdens" were not "sufficient to trigger First Amendment scrutiny." *Id.* at 686.

Further, a business "has no free-floating First Amendment right to 'amass' funds to finance its speech." *Interpipe*, 898 F.3d at 904. So a showing that a business might have to divert resources or lose income as a result of regulation is not sufficient to prove that a regulation should be subject to heightened scrutiny. *ASJA*, 15 F.4th at 962 (labor regulation that might indirectly result in increasing the cost for employers to hire journalists not subject to heightened scrutiny). For example, a regulation that increases the costs of production by requiring worker-safety measures might decrease the money available for advertising. But that advertising is speech subject to heightened scrutiny does not mean that the worker-safety regulation that might result in money being diverted from advertising is subject to heightened scrutiny. *Glickman v. Wileman Bros. & Elliott, Inc.,* 521

U.S. 457, 470 (1997) ("The fact that an economic regulation may indirectly lead to a reduction in a[n] … advertising budget does not itself amount to a restriction on speech.").

b. Only Viewpoint Discriminatory Regulations of Economic Activity Are Subject to Heightened Scrutiny

The prohibition on singling out a speaker or targeting an entity for differential treatment requires more than showing that a particular industry is regulated. *ASJA*, 15 F.4th at 962–633 (rejecting claim that regulation applying to journalists necessarily violates the First Amendment). The Constitution allows—and practicality necessitates—that different industries will sometimes need to be regulated differently. *See, e.g., id.* at 961–62 ("[labor] rules understandably vary based on the nature of the work performed or the industry in which the work is performed"). For example, "a State may choose to regulate price advertising in one industry, but not others, because the risk of fraud … is in its view greater there." *Sorrell,* 564 U.S. at 579 (quotation marks omitted). Where distinctions "make[] sense in light of the objectives of [the law,]" heightened scrutiny is not necessarily warranted. *Interpipe*, 989 F.3d at 903.

The Supreme Court has made the distinction between regulating an industry and targeting a particular speaker many times. In *Arkansas Writers' Project, Inc. v. Ragland*, 481 U.S. 221 (1987), the Court invalidated a state's selective taxation

of certain magazines but not religious, trade, or sports ones. In *Simon & Schuster v. Members of New York State Crime Victims Board*, 502 U.S. 105 (1991), the Court held unconstitutional a law that required publishers of criminals' books to turn over an author's proceeds if the book concerned their crime but allowed other authors to write about the same crime without penalty. On the other hand, laws that regulate an industry without targeting specific speakers within that industry have not been subject to heightened scrutiny. *ASJA*. 15 F.4th at 962–63 (worker classification of freelance journalists was not subject to heightened scrutiny because it did not "target the press or a few speakers" and instead applied "to all freelance writers").

Likewise, "a law affecting entities holding a particular viewpoint is not viewpoint discriminatory unless it targets those entities *because of* their viewpoint." *Interpipe*, 898 F.3d at 900 (emphasis in original). For example, in *Interpipe*, this Court rejected the argument that a state law permitting wage-credits for employee contributions to industry advancement funds only if payments were made pursuant to collective bargaining agreements impermissibly favored union-backed speech. *Id.* at 900–01. As this Court explained, that employees may favor pro-union funds over anti-union funds is "beside the point" because "[a] facially neutral statute restricting expression for a legitimate end is not discriminatory simply because it *affects* some groups more than others." *Id.* at 900 (emphasis in

original). Because the law did not "mandate" differential treatment based on viewpoint, the law was not subject to heightened scrutiny. *Id.*

"[A]bsent narrow circumstances, a court may not conduct an inquiry into legislative purpose or motive beyond what is stated within the statute itself" to determine whether a law is viewpoint discriminatory. *Homeaway.com*, 918 F.3d at 685 (citing *O'Brien*, 391 U.S. 367, 383 n.30 (1968)); *Interpipe*, 898 F.3d at 899 ("If a law is facially neutral, we will not look beyond its text to investigate a possible viewpoint-discriminatory motive.").

2. The Act's Regulation of the Collection and Use of Children's Data Is Not Subject to Heightened Scrutiny

Given these standards, the district court was wrong to apply heightened scrutiny. As an initial matter, the Act regulates economic activity: the collection and use of children's data. As explained above, the record reflects that businesses collect and process children's data so that they can package it and sell it to other companies, retain it and use it to increase profits for their own businesses, or both. 3-ER-392–94; 4-ER-699–701, 704; *see also* 6-ER-1166 (IMDb explaining how data collection and use generates revenue for its business); 7-ER-1191 (same for Goodreads). The information at issue is collected automatically, in great quantities. 3-ER-393–94. Regulating the conditions under which such sale and use can take place falls squarely within the realm of traditional economic activity. *Homeaway.com*, 918 F.3d at 685 ("business agreement[s] or business dealings

[a]re not conduct with a significant expressive element") (internal quotation marks omitted); *FAIR*, 547 U.S. at 66 ("we have extended First Amendment protection only to conduct that is inherently expressive").

Because the collection and sale of data is economic activity, the district court should not have applied heightened scrutiny unless there was an indication of viewpoint discrimination. *Interpipe*, 898 F.3d at 899. And no such viewpoint discrimination exists. The Act does not single out a particular speaker or message for regulation. The Act applies to all for-profit businesses that make over a certain amount of money or trade in a substantial amount of consumer information, and are likely to be accessed by children. §1798.99.30(a) (incorporating definitions from §1798.140); §§1798.99.31(a), (b). Although government and non-profit entities are excluded, such distinctions are permissible. *See ASJA*, 15 F.4th at 963 (a "law is not rendered generally inapplicable just because some other professionals ... enjoy different, or even broader, carve outs"). Government entities and non-profits do not have the same incentives as for-profit businesses to sell and commercially exploit children's data. *See Sorrell*, 564 U.S. at 579 ("a State may choose to regulate price advertising in one industry but not others, because the risk of fraud ... is in its view greater there.") (quotation marks omitted). The law's exclusion for businesses that serve smaller customer-bases likewise makes obvious sense: the number of children affected by a business's data

practices has an obvious relation to the number of children that the business serves. A law with "a legitimate end is not discriminatory simply because it *affects* some groups more than others." *Interpipe*, 898 F.3d at 900. What matters is that the subject of the Act—data collection and use—is "neither expressive nor communicative." *Homeaway.com*, 918 F.3d at 685 ("business agreement[s] or business dealings [a]re not conduct with a significant expressive element").

The Act's limitations on data collection does not "regulate the ingredients necessary to effectuate that entity's First Amendment rights." *Interpipe*, 898 F.3d at 896. Businesses remain free under the Act to express any message. And they can freely express their messages to children. *See ASJA*, 15 F.4th at 961 (no heightened scrutiny to worker classification law where "workers remain able to write, sculpt, paint, design, or market whatever they wish" regardless of classification); *Interpipe*, 898 F.3d at 900–01 (regulations on economic activity are not viewpoint discriminatory where the regulated entities are "—regardless of viewpoint—free to engage in whatever speech they like"). To the extent that businesses *want to* use children's data to express their message, nothing in the First Amendment relieves those businesses of the obligation to obtain and use children's data consistent with the law. *Interpipe*, 898 F.3d at 902–03 (requiring employers to get employee consent before taking a wage-credit for industry advancement fund contributions does not violate the First Amendment).

3. *Sorrell* Does Not Require that Regulations of Data Collection and Use Be Subject to Heightened Scrutiny

The district court believed that *Sorrell* mandates that all regulations of data collection and use be subject to heightened scrutiny. 1-ER-13; 2-ER-98–102. That is incorrect.

Sorrell concerned a Vermont law motivated by legislators' concern that representatives of pharmaceutical manufacturers were, through their presentations, convincing physicians to over-prescribe expensive drugs. 564 U.S. 557–58, 50–61. The pharmaceutical representatives maximized their effectiveness by tailoring their presentations to particular doctors based on those doctors' prescribing practices. *Id.* Vermont's law aimed to stop that by prohibiting the sale, disclosure for marketing purposes, or use for marketing by pharmaceutical manufacturers and drug detailers (people who promote drugs to physicians) of pharmacy records that reveal physicians' prescribing practices. 564 U.S. at 562–63. Other users were not similarly restricted in their ability to access and use that information. *Id.*

The Supreme Court held that under those circumstances, "heightened scrutiny" applied. *Id.* at 565–66, 571. The legislative record and formal legislative findings left no doubt that the legislature "designed" the challenged law to "target" certain "speakers and their messages for disfavored treatment." *Id.* at 565. The law "d[id] not simply have an effect on speech, but [was] directed at certain content and [was] aimed at particular speakers." *Id.* at 567.

If such circumstances were present here, then the application of heightened scrutiny would make sense. But they are not: California's restrictions on the exploitation of children's data do not aim to suppress particular speech or viewpoints. And contrary to the district court's description of the case, 1-ER-12–13, *Sorrell* did not go further and hold that all data collection and use regulations are subject to heightened scrutiny. Indeed, it left open the possibility that prescriber data might be considered "a mere commodity[.]" 564 U.S. at 571. And the Court acknowledged that viewpoint neutral regulations of data sharing might well be constitutional: "The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. In considering how to protect those interests, however, the State cannot engage in content-based discrimination to advance its side of a debate." *Id.* at 579–80.

B. No Other Aspect of the Act Warrants Heightened Scrutiny

1. The Act Does Not Compel Speech

Another reason the district court gave for applying heightened scrutiny was its belief that the Act compels speech. 1-ER-15. That too was incorrect.

The court's compelled speech analysis focused on the Act's requirements that businesses provide their policies including privacy policies and community

standards to child users, and that businesses provide child-users an indication when they are being tracked, 1-ER-15 [,] but Plaintiff's compelled speech arguments focused on the DPIA provision, 5-ER-764–772. None of these provisions should be subject to heightened scrutiny because, to the extent they impact businesses' speech at all, that impact is incidental to the Act's regulation of data collection and use. *FAIR*, 547 U.S. at 62 (alleged "compelled speech" that "is plainly incidental to the [law's] regulation of conduct" is not subject to heightened scrutiny) (citing cases).

As described above, States may regulate economic activity even if that regulation incidentally burdens speech. The key to determining the appropriate level of scrutiny is determining whether the goal of the regulation is regulating speech or whether the impact on speech is incidental to the regulation achieving legitimate goals. *Id.* at 60–62. Here, the Act's DPIA and disclosure requirements are incidental to its legitimate goals of protecting children from excessive data collection and use and thus is not subject to heightened scrutiny.

The DPIA requirement only serves to further the goals of the Act. As explained in detail above, it asks businesses to assess how they are using children's data, how that use might harm children, and how they might mitigate that potential harm. §1798.99.31(a)(1)–(2). There is no penalty or punishment for failing to identify a potential risk or rectify a potential harm identified in the DPIA, although

a business may be penalized if that failure constitutes a violation of a different provision of the Act. *Id.* The role of the DPIA provision is to incentivize businesses to be proactive about their management of children's data by offering businesses that complete the DPIA a 90-day period to cure violations of the Act without penalty, §1798.99.35(c). *Interpipe*, 898 F.3d at 896 (distinguishing between incentivizing conduct and regulating speech). The DPIA does not compel businesses to express a message or interfere with any message a business might wish to send. *FAIR*, 547 U.S. at 64 (requirement that law schools treat military recruiters identically to other recruiters "is not compelled speech because the accommodation does not sufficiently interfere with any message of the school"). And it is not subject to public disclosure. §1798.99.31(a)(4)(B). Even if the Attorney General requests to review a DPIA—which may never happen—it remains confidential and privileged. §1798.99.31(a)(4)(C).

Additionally, the DPIA is a reporting requirement that falls well within the bounds of appropriate government regulation that is not traditionally subject to heightened scrutiny. *See Hotel Emps. & Rest. Emps. Int'l Union v. Nev. Gaming Comm'n*. 984 F.2d 1507, 1518 (9th Cir. 1993); *Village of Schaumburg v. Citizens for a Better Env't*, 444 U.S. 620, 637–38 & n.12 (1980) (requirement to "report certain information" on a routine basis is permissible); *see also*, *e.g.,* 26 U.S.C.

§501(r)(3) (non-profit hospitals must conduct community health needs assessment every three years and adopt implementation strategy to meet identified needs).

The requirements that businesses provide child-users information about any policies the business may have that explain how their data is being used is likewise incidental to the Act's goal of protecting children from excessive data collection and use. Children and parents need to know and understand how businesses are using their data to be able to consent to it. 3-ER-400, 405. The Act only requires that a businesses' policies—if they exist and whatever they are—be published in language that child-users understand, §1798.99.31(a)(7). *See FAIR*, 547 U.S. at 60 (law "regulates conduct, not speech" where "[i]t affects what [regulated entities] must *do* ... not what they may or may not *say*") (emphasis in orginal). That the Act also requires businesses to enforce their own policies does not change the analysis. The Act in no way requires businesses to have such policies or dictates the content of such polices, and thus does not compel speech. *Id.*

Further, even if the Act's disclosure requirements were subject to the scrutiny applied to compelled speech, they would survive it. Businesses can be "required to 'disclose factual, noncontroversial information,' such as the terms under which professional services are offered." *Tingley v. Ferguson*, 47 F.4th 1055, 1074 (9th Cir. 2022) (citing *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2372 (2018)). Businesses' privacy policies, terms of use, community

standards, and information concerning whether a child-user is being tracked constitute such factual noncontroversial information. *Envtl. Def. Ctr., Inc. v. U.S. E.P.A.*, 344 F.3d 832, 849 (9th Cir. 2003) (factual and uncontroversial requirement is satisfied where law does not "attempt[] to 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 threin"); *Nationwide Biweekly Admin., Inc. v. Owen*, 873 F.3d 716, 732 (9th Cir. 2017) ("[u]ncontroversial ... refers to the factual accuracy of the compelled disclosure, not to its subjective impact on the audience[]"). These provisions are rationally related to the State's legitimate goal of protecting children from excessive data collection and use, thus they do not violate the First Amendment. *Owen*, 873 F.3d at 721 ("The First Amendment does not generally protect corporations from being required to tell prospective customers the truth.").

2. The Act Does Not Restrict the First Amendment Rights of Internet Users

The district court's opinion relies heavily on Plaintiff's contention that the Act would infringe on the rights of internet *users* to obtain information. *See, e.g.,* 1-ER-16. But no users are plaintiffs here, and the district court opinion contains no analysis at all of why users' rights are cognizable in NetChoice's suit under third-party standing doctrine. *Cf.* 1-ER-7; 2-ER-79 (court suggesting "looking at the effect on users, such as the children, would be beyond the scope of the standing

requirements"); 2-ER-139 (court stating "I'm not sure I can jump to the harm to users under even a relaxed standing requirements for a facial attack under the First Amendment"). Moreover, the order erroneously states that Defendant did not oppose the court's consideration of third-party rights. 1-ER-7. As the court acknowledged at hearing, 2-ER-79, Defendant raised the inappropriateness of Plaintiff raising third-party claims in briefing. 3-ER-371 (citing *Marquez-Reyes v. Garland*, 36 F.4th 1195, 1201 (9th Cir. 2022)). In any event, Plaintiff certainly made no effort to show that the requirements for asserting another party's rights were met in this case. To assert third-party standing "[t]he litigant must have suffered an 'injury in fact,' thus giving him or her a 'sufficiently concrete interest' in the outcome of the issue in dispute; the litigant must have a close relationship to the third party; and there must exist some hindrance to the third party's ability to protect his or her own interest." *Coal. of Clergy, Lawyers & Professors v. Bush*, 310 F.3d 1153, 1163 (9th Cir. 2002) (quoting *Powers v. Ohio*, 499 U.S. 400, 410–411) (1991)). Indeed, there are multiple ways in which the interests of websites that harvest personal data for profit differ from the interest of those children whose data is harvested. *See, e.g.,* 4-ER-686–691.

Nor was there a basis to conclude that the Act would infringe on internet users' rights. Plaintiff argues that the Act will cause services to shut down or to exclude some users. 5-ER-878–79. The culprit, according to Plaintiff, is the Act's

requirement that businesses either estimate the age of child-users or apply the data and privacy protections afforded to child-users to all users. *Id.* According to Plaintiff, age-estimation is so invasive and expensive as to be impossible or impractical, and the alternative of providing protections to all users would be economically impossible given their business models. *Id.*; 6-ER-1166 (IMDb explaining how data collection and use generates revenue for its business); 7-ER-1191 (same for Goodreads).

But plaintiffs' support for these claims fell woefully short. Plaintiff proffered no expert evidence about the feasibility of age estimation methods. And relied on grossly outdated cases, which commented on age-estimation methods that were available *ten to twenty years ago*. 5-ER-878–79 (citing out of circuit cases decided between 1999 and 2008). In a fast-moving field like computer technology, such evaluations from long ago carry little weight. As Defendant's experts explained, age estimation is both viable and practical. 4-ER-709–11; 3-ER-411–12. Multiple technologies exist for estimating age. *Id.* Indeed, many companies, including some NetChoice members, currently remove child accounts (who provided a false birthday when signing up) using information the companies already have. 4-ER-710. Businesses can contract with third-parties that are using existing technologies that "could easily be used to prove to relying online services that a user is above or below the age of 18 without revealing additional personal information about that

user." 3-ER-411–12. Moreover, NetChoice members are already obligated to comply with COPPA, which requires businesses to estimate whether users are over or under 13. 15 U.S.C. §§6501–6506; 16 C.F.R. §312.2. The district court's assumption that age estimation is impossible or impractical relied not on record evidence but on speculative arguments in amicus briefs. 1-ER-16, 23–24, 29–30. But an amicus brief is not *evidence*. *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 434 n.16 (1984) ("The stated desires of *amici* concerning the outcome of this or any litigation are ... not evidence in the case, and do not influence our decision; we examine an *amicus curiae* brief solely for whatever aid it provides in analyzing the legal questions before us.")

Nor does the district court's conclusion constitute a finding of fact— and in any event a finding based on no evidence would be clearly erroneous. *Oregon Nat. Res. Counsel v. Marsh*, 52 F.3d 1485, 1492 (9th Cir. 1995). As importantly, the district court violated this Court's instruction that a finding of likelihood of success must be based on actual fact-based evidence, not hypothetical scenarios. *Thomas v. Anchorage Equal Rights Comm'n*, 220 F.3d 1134, 1141–42 (9th Cir. 2000) (en banc) (First Amendment challenge rejected where "the entire argument about the effect of the ... statute rest[ed] upon hypothetical situations with hypothetical clients" and was "devoid of any specific factual context"); *Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1126 (9th Cir. 2009) (First Amendment challenges cannot

be based on "incomplete hypotheticals or open factual questions akin to those in *Thomas*"). It should be reversed.

II. THE ACT SATISFIES THE *CENTRAL HUDSON* STANDARD FOR A CONSTITUTIONAL COMMERCIAL SPEECH REGULATION.

As explained above, heightened scrutiny does not apply. But if it did, the Act would still be constitutional. The Supreme Court has "afforded commercial speech a limited measure of protection, commensurate with its subordinate position in the scale of First Amendment values, while allowing modes of regulation that might be impermissible in the realm of noncommercial expression." *Ohralik*, 436 U.S. at 456.

The governing test is the four-step analysis of *Central Hudson Gas & Electric Corp. v. Public Service Commission*, 447 U.S. 557 (1980). First, for heightened scrutiny to apply, the speech "must concern lawful activity and not be misleading." *Id.* at 566. Second, the governmental interest must be "substantial." *Id.* Assuming these first two requirements are met, then third, the court determines "whether the regulation directly advances the government interest asserted[.]" *Id.* Last, the court determines whether the regulation is "not more extensive than necessary to serve that interest." *Id.* As the Supreme Court has clarified, this last step is not a least-restrictive-means test. *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 556 (2001). The means need "not necessarily [be] the single best disposition but one whose scope is in proportion to the interest served[.]" *Bd. of Trustees of State Univ.*

of N.Y. v. Fox, 492 U.S. 469, 480 (1989) (internal quotation marks omitted). Courts "leave it to governmental decisionmakers to judge what manner of regulation may best be employed." *Id.*

Although the parties differ on the last three Central Hudson requirements, the Act in fact satisfies them all.[5] California's interest in protecting children from such harms as having their location tracked by strangers or made available for sale, being targeted for manipulative advertising, or being pushed knowingly harmful and unwanted material, such as videos promoting self-harm, are indeed substantial. The Act directly advances those interests, by methods such as restricting the use of geolocation data, §§1798.99.31(b)(5)–(6), prohibiting unnecessary profiling, §1798.99.31(b)(2), ensuring that privacy information is provided to children in a form they can understand, §1798.99.31(a)(7), and providing privacy protections by default, §1798.99.31(a)(6). And the Act includes multiple safeguards to ensure that the fit between those means and the goals served is adequate. For instance, the Act regulates only websites with a profit motive that will make them susceptible to

[5] The first Central Hudson requirement, that the act concern lawful activity and not be misleading, is not, strictly speaking, a requirement for passing the *Central Hudson* test. Instead, where this requirement is not met (because the commercial speech is misleading or solicits law-breaking), an even lower standard of scrutiny applies. *In re R.M.J.*, 455 U.S. 191, 203 (1982) ("Misleading advertising may be prohibited entirely.") This prong is only at issue in this case with respect to the requirement that platforms enforce their published policies, §1798.99.31(a)(9): to the extent a stated policy misleads the public, regulation of that misstatement would fail to meet the first step of *Central Hudson*.

abusing children's information and a size that would make such abuses potentially widespread, §1798.99.30(a) (incorporating definitions from §1798.140); it safeguards information in DPIAs from public disclosure, §1798.99.31(a)(4)(B); it avoids any private right of action for violations, §1798.99.35(d), and provides companies with notice-and-cure protections before the Attorney General can sue. §1798.99.35(c). Moreover, Defendant supported its explanation of this fit with detailed expert declarations, and the Act is modeled on a U.K. enactment whose effects those experts described in detail. 3-ER-389–431; 4-ER-677–740; 3-ER-343–455. In finding the law unconstitutional nonetheless, the district court made errors with respect to each provision it evaluated.

The district court made multiple errors when evaluating whether the State's methods of regulation advanced its interests. In perhaps the most egregious example, the court invalidated a requirement that businesses likely to be accessed by children must provide their user policies using age-appropriate language, §1798.99.31(a)(7), because it found there was no evidence that children would not understand policies written at the college level. 1-ER-26–27. The court further concluded that even if there were such evidence, the State did not prove that providing policies that a child would understand, including privacy policies, would aid children in protecting their data. *Id.* However, Defendant provided two detailed expert declarations detailing minors' experiences with current business

practices and how the Act addresses those harms, and a third declaration describing how a nearly identical Act in the U.K. is alleviating these harms. 3-ER-392–416, 432–455; 4-ER-683–702, 705–712. And even without that evidence, the conclusion that providing children with policies they can understand will help them would suffice as a matter of common sense. *See Fla. Bar v. Went For It, Inc.*, 515 U.S. 618, 628 (1995) (restrictions may be "based solely on history, consensus, and simple common sense") (internal quotation marks omitted).

At other times, the district court erroneously required the State to prove that the provisions of the Act completely eradicate any potential harm the provision was designed to address. *See, e.g.*, 1-ER-22 (invalidating DPIA requirement). But that circumstances that detract from the State's asserted interest continue to exist in spite of regulation does not defeat the State's interest. *Coyote Pub. Inc. v. Miller*, 598 F.3d 592, 609 (9th Cir. 2010) (Nevada's ban on advertising prostitution advances its interest in limiting the commodification of sex even though it could have advanced that interest further by banning prostitution altogether). Such a standard would subvert the Legislature's power to "str[ike] its own idiosyncratic balance between various important but competing state interests" when crafting provisions. *Id.* at 606. For example, the court invalidated the requirement that businesses estimate the age of child users or provide the privacy and data protection afforded to minors to all users, §1798.99.31(a)(5), because it concluded

that age estimation "appear[s] to counter the State's interest in increasing privacy protections for children." 1-ER-24. It likewise invalidated the prohibition on businesses profiling children by default, §1798.99.31(b)(2), because it concluded that it "may" result in some children "hav[ing] a more difficult time finding resources[.]" 1-ER-30. And the court invalidated the requirement that businesses complete a Data Protection Impact Assessment, §1798.99.31(a)(1), because "it do[es] not require businesses to assess the potential harm of the design of digital [services] and also doe[es] not require actual mitigation of any identified risks[.]" 1-ER-22. The court invalidated all of these provisions based on its own assessment that other methods might better advance the State's interest, but *Central Hudson* does not allow a court to invalidate a law on that basis. That another method of regulation might also promote the same interest "does not by itself render a commercial speech regulation unconstitutional." *Coyote Pub.*, 598 F.3d at 608. "To so hold would be tantamount to requiring that government utilize the least speech restrictive means, which the Supreme Court has made clear is not a *sine qua non* under *Central Hudson*." *Id.* at 609.

Here, the Act clearly advances the State's interest in protecting children's privacy and safety, and none of the possible scenarios identified by the court detract from the advancement of that interest. These provisions are part of the Legislature's "delicate compromise among competing issues and concerns." *In re*

Welsh, 711 F.3d 1120, 1133 ("declin[ing] to give greater weight to one of the purposes of" the challenged law) (quotation marks omitted). For example, the Legislature understood that age estimation could potentially require data collection—that is why the Act requires age estimation tools be "minimally invasive[,]"§1798.99.32(d)(3), and that any data collected for age estimation be used only for that purpose, §1798.99.31(b)(8)[6]—but it made the calculation that the benefits of age-appropriate privacy and data protections would be worth the limited intrusion. Likewise, the Legislature understood that limiting profiling would result in children having a more self-directed experience online, and it is within the Legislature's purview to determine that a prohibition on profiling with limited exceptions, §1798.99.31(b)(2), creates the appropriate balance between encouraging a self-directed experience and allowing some profiling when it is in the best interest of the child. With the DPIA requirement, the Legislature chose to incentivize regulated businesses to identify risks and mitigate harm by giving businesses that comply with the DPIA requirement a 90-day period to cure violations without penalties. §1798.99.35(c).

[6] Despite the clear language in the statute, the district court assumed—without evidence—that the Act *requires* businesses to use invasive means to estimate age. 1-ER-23–24. This conclusion is unsupported by fact. On its face, the Act does not require the use of invasive age estimation tools—the Act explicitly discourages their use, §1798.99.32(d)(3), —and Plaintiff has not proven that such tools will be required in practice.

In short, what the district court identified as flaws in the Act are actually carefully considered compromises that, in the Legislature's judgement, best advance the State's interest. "The First Amendment does not require that the regulatory regime single-mindedly pursue one objective to the exclusion of all others to survive the intermediate scrutiny applied to commercial speech regulations." *Coyote Pub.*, 598 F.3d at 610. Rather, a States is permitted to "strike[] a balance between its interest[s]." *Id.*

Likewise, the court erred in invalidating provisions based on its conclusion that prohibitions on the collection and use of data might lead to harmful as well as beneficial outcomes for children. *See* 1-ER-29–32 (invalidating provisions restricting knowingly harmful data use (§1798.99.31(b)(1)), profiling (§1798.99.31(b)(2)), and unnecessary collection, sale, sharing, retention, and use of children's data (§1798.99.31(b)(3)), because they "thow[] out the baby with the bathwater"). In addition to depriving the Legislature of its ability to strike the right balance in determining the best way to address the problems facing its most vulnerable constituents, *see infra*, applying such a test would leave the Legislature in the position where it could only address problems in the way that federal courts deem to be the perfect fit, a clear contradiction of what intermediate scrutiny requires. *Contest Promotions, LLC, v. City & County of San Francisco*, 874 F.3d 597, 604 (9th Cir. 2017) ("It is well established that a law need not deal perfectly

and fully with an identified problem to survive intermediate scrutiny."); *see also Coyote Pub.,* 598 F.3d at 611 (Noonan, concurring) ("the state may take a half-step").

The court also committed several errors in determining that the means used to advance the State's interest are more excessive than necessary. Many of these errors occurred because the district court's analysis is based on a clear misreading of the Act. For example, it concluded that the requirement that businesses enforce their own published policies, §1798.99.31(a)(9), is not restricted to children, 1-ER-28, when, on its face, the Act only applies to businesses that offer services, products, and features likely to be accessed by children, §1798.99.31(a), (b), and penalties are assessed based on the number of children harmed by violations, §1798.99.35(a).

The court also repeatedly erred by basing its conclusions about whether the Act's methods are more extensive than necessary on Plaintiff's and amici's speculation that businesses will have an extreme reaction to regulation, rather than on the terms of the Act itself. Plaintiff speculated that businesses might choose to limit content, block child users, or stop providing services entirely rather than comply with the Act. 5-ER-878–79. The court then used this speculation as a basis to invalidate a number of provisions, including the requirement that businesses either estimate user age or provide the privacy and data protections

afforded to children to all users, §1798.99.31(a)(5), and the requirement that children be provided high-privacy settings by default, §1798.99.31(a)(6). 1-ER-22–26. It invalidated the prohibition on businesses using children's data in ways that the business knows will harm children, §1798.99.31(b)(1), concluding, based on amici's assertions, that "businesses might well bar all children from accessing their online services rather than" comply with the Act. 1-ER-29–30; *See also* 1-ER-35 (invalidating prohibition on businesses using dark patterns, §1798.99.31(b)(7), because it concluded, based on amici's assertions, that the provision "may cause covered businesses to deny children access to their platforms or content")

Businesses may choose to limit content, block children, treat all users as children, or shut down entirely rather than comply with the Act, but these are not required outcomes or inevitable results of the Act. *See Homeaway,* 918 F.3d at 685–86 (courts must look at the "inevitable effect of the [Act] in its face" when evaluating First Amendment claims). Such speculation cannot be the basis for a determination that the *Act* is more extensive than necessary or for facially invalidating it. *See, e.g., Thomas*, 220 F.3d at 1141–42; *Stormans*, 586 F.3d at 1126.

The Act restricts businesses' collection and use of children's data in specific and circumscribed ways that narrowly target excessive data collection and use that

pose risks to children. Under the plain terms of the Act, businesses can continue to provide whatever services they want to whichever users they want. Thus, the Act does not use methods more extensive than necessary to advance the State's interest.

III. THE ACT IS SEVERABLE

After the First Amendment analysis, the district court concluded that "two mandates; three prohibitions, and provisions establishing a working group" and "penalties for violating the Act" were the remaining substantive provisions. 1-ER-37. The district court erroneously invalidated all of these provisions upon a finding that they were not severable. 1-ER-35–38.

The Act itself does not create an assumption for or against severability. *See Garcia v. City of Los Angeles*, 11 F.4th 1113, 1120 (9th Cir. 2021) (absent a severability clause, no assumptions apply). In such a case, to determine severability, this Court must apply California law, which evaluates three factors: grammatical, functional, and volitional severability. *Id.*

Here, all three factors weigh in favor of severability. The remaining provisions are "distinct and separate" from the invalidated provisions. *Calfarm Ins. Co. v. Deukmejian*, 771 P.2d 1247, 1256 (Cal. 1989).; *see also County Org. of Public Employees v. County of Sonoma*, 591 P.2d 1, 14–15 (Cal. 1979) (applying severability analysis). And the court did not find otherwise. Although the court

invalidated the DPIA provision, which, in turn, would eliminate the cure period, the remaining provisions remain exactly the same. Each provision of the Act operates independently without reliance on the language in, or businesses' compliance with, other provisions. For example, a businesses can still provide prominent, accessible, and responsive tools to help children exercise their privacy rights and report concerns, §1798.99.31(a)(10), or provide an obvious signal to child users when they are being tracked, §1798.99.31(a)(8), even if the business did not complete a DPIA and even if no cure period is available.

The Act is also volitionally severable. It passed unanimously and there is "no persuasive reason to suppose that [the invalidated provisions] w[ere] so critical to the enactment of [the Act] that the measure would not have been enacted in [their] absence." *Deukmejian*, 771 P.2d at 1256. Indeed, the opposite is true. Given the important and urgent need and overwhelming support for increasing children's data privacy protections, "it seems eminently reasonable to suppose that those who favor the proposition would be happy to achieve at least some substantial portion of their purpose" by requiring businesses to take important steps such as reducing tracking of children online and establishing a working group to recommend best practices for children's privacy. *Santa Barbara Sch. Dist. v. Superior Court*, 530 P.2d 605, 618 (Cal. 1975) (in bank). Thus, the remaining provisions are

grammatically, functionally, and volitionally severable from any invalidated provisions.

CONCLUSION

The injunction should be vacated.

Dated: December 13, 2023

Respectfully submitted,

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

s/ Elizabeth Watson
ELIZABETH WATSON
Deputy Attorney General
Attorneys for Defendant

SA2023305531

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 17. Statement of Related Cases Pursuant to Circuit Rule 28-2.6

Instructions for this form: http://www.ca9.uscourts.gov/forms/form17instructions.pdf

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

The undersigned attorney or self-represented party states the following:

- (•) I am unaware of any related cases currently pending in this court.
- ( ) I am unaware of any related cases currently pending in this court other than the case(s) identified in the initial brief(s) filed by the other party or parties.
- ( ) I am aware of one or more related cases currently pending in this court. The case number and name of each related case and its relationship to this case are:

Signature s/ Elizabeth K. Watson **Date** Dec 13, 2023

*(use "*s/[typed name]*" to sign electronically-filed documents)*

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 11,025 **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/ Elizabeth K. Watson **Date** Dec. 13, 2023
*(use "*s/[typed name]*" to sign electronically-filed documents)*

CERTIFICATE OF SERVICE

Case Name: **NetChoice, LLC v Rob Bonta** No. **23-2969 [Appeal]**

I hereby certify that on December 13, 2023, I electronically filed the following documents with the Clerk of the Court by using the CM/ECF system:

APPELLANT'S OPENING BRIEF

Participants in the case who are registered CM/ECF users will be served by the CM/ECF system.

I am employed in the Office of the Attorney General, which is the office of a member of the California State Bar at which member's direction this service is made. I am 18 years of age or older and not a party to this matter. I am familiar with the business practice at the Office of the Attorney General for collection and processing of correspondence for mailing with the United States Postal Service. In accordance with that practice, correspondence placed in the internal mail collection system at the Office of the Attorney General is deposited with the United States Postal Service with postage thereon fully prepaid that same day in the ordinary course of business.

I further certify that some of the participants in the case are not registered CM/ECF users. On December 13, 2023, I have caused to be mailed in the Office of the Attorney General's internal mail system, the foregoing document(s) by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within three (3) calendar days to the following non-CM/ECF participants:

District Judge Beth Labson Freeman
San Jose Courthouse, Courtroom 3 – 5th Floor
280 South 1st Street
San Jose, CA 95113

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 and that this declaration was executed on December 13, 2023, at Los Angeles, California.

J. Sissov	/s/ *J. Sissov*
Declarant	Signature

SA2023305531

23-2969

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

NETCHOICE, LLC, Appellee, **v.** **ROB BONTA,** 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

ADDENDUM

ROB BONTA
Attorney General of California
THOMAS S. PATTERSON
Senior Assistant Attorney General
ANYA M. BINSACCA
Supervising Deputy Attorney General
ELIZABETH WATSON
Deputy Attorney General
State Bar No. 295221
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3847
Email: Elizabeth.Watson@doj.ca.gov
Attorneys for Defendant-Appellant

TABLE OF CONTENTS

Page

Assembly Bill No. 2273

CHAPTER 320

An act to add Title 1.81.47 (commencing with Section 1798.99.28) to Part 4 of Division 3 of, and to repeal Section 1798.99.32 of, the Civil Code, relating to consumer privacy.

[Approved by Governor September 15, 2022. Filed with Secretary of State September 15, 2022.]

LEGISLATIVE COUNSEL'S DIGEST

AB 2273, Wicks. The California Age-Appropriate Design Code Act.

(1) Existing law, the California Privacy Rights Act of 2020, approved by the voters as Proposition 24 at the November 3, 2020, statewide general election, establishes the California Privacy Protection Agency. Existing law vests the agency with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018 and requires the agency to be governed by a board. Existing law requires businesses to protect consumer privacy and information, make certain disclosures to consumers regarding a consumer's rights under the act in a specified manner, and disclose to consumers that a consumer has the right to request specific pieces of information, including the categories of information those businesses have collected about that consumer.

Existing law, the Parent's Accountability and Child Protection Act, requires a person or business that conducts business in California and that seeks to sell specified products or services to take reasonable steps to ensure that the purchaser is of legal age at the time of purchase or delivery, including verifying the age of the purchaser. Existing law prohibits a person or business that is required to comply with these provisions from retaining, using, or disclosing any information it receives in an effort to verify age from a purchaser or recipient for any other purpose, except as specified, and subjects a business or person that violates these provisions to a civil penalty.

This bill would enact the California Age-Appropriate Design Code Act, which, commencing July 1, 2024, would, among other things, require a business that provides an online service, product, or feature likely to be accessed by children to comply with specified requirements, including a requirement to configure all default privacy settings offered by the online service, product, or feature to the settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children, and to provide privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature. The bill would require a business, before any new online services, products, or features are offered to the public, to

complete a Data Protection Impact Assessment, as defined, for any online service, product, or feature likely to be accessed by children and maintain documentation of this assessment as long as the online service, product, or feature is likely to be accessed by children. The bill would require a business to make a Data Protection Impact Assessment available, within 5 business days, to the Attorney General pursuant to a written request and would exempt a Data Protection Impact Assessment from public disclosure, as prescribed. The bill would prohibit a business that provides an online service, product, or feature likely to be accessed by children from taking proscribed action, including, if the end user is a child, using personal information for any reason other than a reason for which the personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children.

This bill would create the California Children's Data Protection Working Group to deliver a report to the Legislature regarding best practices for the implementation of these provisions, as specified. The bill would require the members of the working group to have certain expertise, including in the areas of children's data privacy and children's rights. The bill would require the working group to take input from a broad range of stakeholders, including from academia, consumer advocacy groups, and small, medium, and large businesses affected by data privacy policies, and make prescribed recommendations on best practices, including identifying online services, products, or features likely to be accessed by children.

This bill would authorize the Attorney General to seek an injunction or civil penalty against any business that violates its provisions. The bill would hold violators liable for a civil penalty of not more than $2,500 per affected child for each negligent violation or not more than $7,500 per affected child for each intentional violation. The bill would require any penalties, fees, and expenses recovered in an action brought under the act to be deposited in the Consumer Privacy Fund with the intent that they be used to fully offset costs incurred by the Attorney General in connection with the act.

(2) The California Privacy Rights Act of 2020 authorizes the Legislature to amend the act to further the purposes and intent of the act by a majority vote of both houses of the Legislature, as specified.

This bill would declare that its provisions further the purposes and intent of the California Privacy Rights Act of 2020.

(3) Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.

This bill would make legislative findings to that effect.

The people of the State of California do enact as follows:

SECTION 1. (a) The Legislature hereby finds and declares all of the following:

(1) The United Nations Convention on the Rights of the Child recognizes that children need special safeguards and care in all aspects of their lives.

(2) As children spend more of their time interacting with the online world, the impact of the design of online products and services on children's well-being has become a focus of significant concern.

(3) There is bipartisan agreement at the international level, in both the United States and in the State of California, that more needs to be done to create a safer online space for children to learn, explore, and play.

(4) Lawmakers around the globe have taken steps to enhance privacy protections for children on the understanding that, in relation to data protection, greater privacy necessarily means greater security and well-being.

(5) Children should be afforded protections not only by online products and services specifically directed at them, but by all online products and services they are likely to access. In order to help support the design of online products, services, and features, businesses should take into account the unique needs of different age ranges, including the following developmental stages: 0 to 5 years of age or "preliterate and early literacy"; 6 to 9 years of age or "core primary school years"; 10 to 12 years of age or "transition years"; 13 to 15 years of age or "early teens"; and 16 to 17 years of age or "approaching adulthood."

(6) In 2019, 81 percent of voters said they wanted to prohibit companies from collecting personal information about children without parental consent, and a 2018 poll of Californian parents and teens found that only 36 percent of teenagers and 32 percent of parents say that social networking internet websites do a good job explaining what they do with users' data.

(7) While it is clear that the same data protection regime may not be appropriate for children of all ages, children of all ages should nonetheless be afforded privacy and protection, and online products and services should adopt data protection regimes appropriate for children of the ages likely to access those products and services.

(8) Online services, products, or features that are likely to be accessed by children should offer strong privacy protections by design and by default, including by disabling features that profile children using their previous behavior, browsing history, or assumptions of their similarity to other children, to offer detrimental material.

(9) Ensuring robust privacy protections for children by design is consistent with the intent of the Legislature in passing the California Consumer Privacy Act of 2018, and with the intent of the people of the State of California in passing the California Privacy Rights Act of 2020, which finds and declares that children are particularly vulnerable from a negotiating perspective with respect to their privacy rights.

(10) The California Privacy Protection Agency, created by the California Privacy Rights Act of 2020, has substantial and growing expertise that is integral to the development of privacy policy in California.

(b) Therefore, it is the intent of the Legislature to promote privacy protections for children pursuant to the California Age-Appropriate Design Code Act.

(c) It is the intent of the Legislature that the California Age-Appropriate Design Code promote innovation by businesses whose online products, services, or features are likely to be accessed by children by ensuring that those online products, services, or features are designed in a manner that recognizes the distinct needs of children at different age ranges.

(d) It is the intent of the Legislature that businesses covered by the California Age-Appropriate Design Code may look to guidance and innovation in response to the Age-Appropriate Design Code established in the United Kingdom when developing online services, products, or features likely to be accessed by children.

(e) It is the intent of the Legislature that the California Children's Data Protection Working Group consider the guidance provided by the Information Commissioner's Office in the United Kingdom when developing and reviewing best practices or other recommendations related to the California Age-Appropriate Design Code.

(f) It is the intent of the Legislature that the California Children's Data Protection Working Group and the Department of Justice leverage the substantial and growing expertise of the California Privacy Protection Agency in the implementation of this title.

SEC. 2. Title 1.81.47 (commencing with Section 1798.99.28) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.47. THE CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT

1798.99.28. This title shall be known, and may be cited, as the California Age-Appropriate Design Code Act.

1798.99.29. The Legislature declares that children should be afforded protections not only by online products and services specifically directed at them but by all online products and services they are likely to access and makes the following findings:

(a) Businesses that develop and provide online services, products, or features that children are likely to access should consider the best interests of children when designing, developing, and providing that online service, product, or feature.

(b) If a conflict arises between commercial interests and the best interests of children, companies should prioritize the privacy, safety, and well-being of children over commercial interests.

1798.99.30. (a) For purposes of this title, the definitions in Section 1798.140 shall apply unless otherwise specified in this title.

(b) For the purposes of this title:

(1) "Child" or "children," unless otherwise specified, means a consumer or consumers who are under 18 years of age.

(2) "Data Protection Impact Assessment" means a systematic survey to assess and mitigate risks that arise from the data management practices of the business to children who are reasonably likely to access the online

service, product, or feature at issue that arises from the provision of that online service, product, or feature.

(3) "Default" means a preselected option adopted by the business for the online service, product, or feature.

(4) "Likely to be accessed by children" means it is reasonable to expect, based on the following indicators, that the online service, product, or feature would be accessed by children:

(A) The online service, product, or feature is directed to children as defined by the Children's Online Privacy Protection Act (15 U.S.C. Sec. 6501 et seq.).

(B) The online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children.

(C) An online service, product, or feature with advertisements marketed to children.

(D) An online service, product, or feature that is substantially similar or the same as an online service, product, or feature subject to subparagraph (B).

(E) An online service, product, or feature that has design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children.

(F) A significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.

(5) "Online service, product, or feature" does not mean any of the following:

(A) A broadband internet access service, as defined in Section 3100.

(B) A telecommunications service, as defined in Section 153 of Title 47 of the United States Code.

(C) The delivery or use of a physical product.

(6) "Profiling" means any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

1798.99.31. (a) A business that provides an online service, product, or feature likely to be accessed by children shall take all of the following actions:

(1) (A) Before any new online services, products, or features are offered to the public, complete a Data Protection Impact Assessment for any online service, product, or feature likely to be accessed by children and maintain documentation of this assessment as long as the online service, product, or feature is likely to be accessed by children. A business shall biennially review all Data Protection Impact Assessments.

(B) The Data Protection Impact Assessment required by this paragraph shall 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. The

Data Protection Impact Assessment shall address, to the extent applicable, all of the following:

(i) 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.

(ii) Whether the design of the online product, service, or feature could lead to children experiencing or being targeted by harmful, or potentially harmful, contacts on the online product, service, or feature.

(iii) Whether the design of the online product, service, or feature could permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct on the online product, service, or feature.

(iv) Whether the design of the online product, service, or feature could allow children to be party to or exploited by a harmful, or potentially harmful, contact on the online product, service, or feature.

(v) Whether algorithms used by the online product, service, or feature could harm children.

(vi) Whether targeted advertising systems used by the online product, service, or feature could harm children.

(vii) Whether and how the online product, service, or feature uses system design features to increase, sustain, or extend use of the online product, service, or feature by children, including the automatic playing of media, rewards for time spent, and notifications.

(viii) Whether, how, and for what purpose the online product, service, or feature collects or processes sensitive personal information of children.

(2) Document any risk of material detriment to children that arises from the data management practices of the business identified in the Data Protection Impact Assessment required by paragraph (1) and create a timed plan to mitigate or eliminate the risk before the online service, product, or feature is accessed by children.

(3) Within three business days of a written request by the Attorney General, provide to the Attorney General a list of all Data Protection Impact Assessments the business has completed.

(4) (A) For any Data Protection Impact Assessment completed pursuant to paragraph (1), make the Data Protection Impact Assessment available, within five business days, to the Attorney General pursuant to a written request.

(B) Notwithstanding any other law, a Data Protection Impact Assessment is protected as confidential and shall be exempt from public disclosure, including under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code).

(C) To the extent any information contained in a Data Protection Impact Assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, disclosure pursuant to this paragraph shall not constitute a waiver of that privilege or protection.

(5) Estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of

the business or apply the privacy and data protections afforded to children to all consumers.

(6) Configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.

(7) Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature.

(8) If the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, provide an obvious signal to the child when the child is being monitored or tracked.

(9) Enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.

(10) Provide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns.

(b) A business that provides an online service, product, or feature likely to be accessed by children shall not take any of the following actions:

(1) Use the personal information of any child in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child.

(2) Profile a child by default unless both of the following criteria are met:

(A) The business can demonstrate it has appropriate safeguards in place to protect children.

(B) Either of the following is true:

(i) Profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged.

(ii) The business can demonstrate a compelling reason that profiling is in the best interests of children.

(3) Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, or as described in paragraphs (1) to (4), inclusive, of subdivision (a) of Section 1798.145, unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of children likely to access the online service, product, or feature.

(4) If the end user is a child, use personal information for any reason other than a reason for which that personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children.

(5) Collect, sell, or share any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary for the business to provide the service, product, or feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature.

(6) Collect any precise geolocation information of a child without providing an obvious sign to the child for the duration of that collection that precise geolocation information is being collected.

(7) Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being.

(8) Use any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age. Age assurance shall be proportionate to the risks and data practice of an online service, product, or feature.

(c) (1) A Data Protection Impact Assessment conducted by a business for the purpose of compliance with any other law complies with this section if the Data Protection Impact Assessment meets the requirements of this title.

(2) A single data protection impact assessment may contain multiple similar processing operations that present similar risks only if each relevant online service, product, or feature is addressed.

(d) This section shall become operative on July 1, 2024.

1798.99.32. (a) The California Children's Data Protection Working Group is hereby created to deliver a report to the Legislature, pursuant to subdivision (e), regarding best practices for the implementation of this title.

(b) Working Group members shall consist of Californians with expertise in at least two of the following areas:

(1) Children's data privacy.

(2) Physical health.

(3) Mental health and well-being.

(4) Computer science.

(5) Children's rights.

(c) The working group shall select a chair and a vice chair from among its members and shall consist of the following 10 members:

(1) Two appointees by the Governor.

(2) Two appointees by the President Pro Tempore of the Senate.

(3) Two appointees by the Speaker of the Assembly.

(4) Two appointees by the Attorney General.

(5) Two appointees by the California Privacy Protection Agency.

(d) The working group shall take input from a broad range of stakeholders, including from academia, consumer advocacy groups, and small, medium, and large businesses affected by data privacy policies and

shall make recommendations to the Legislature on best practices regarding, at minimum, all of the following:

(1) Identifying online services, products, or features likely to be accessed by children.

(2) Evaluating and prioritizing the best interests of children with respect to their privacy, physical health, and mental health and well-being and evaluating how those interests may be furthered by the design, development, and implementation of an online service, product, or feature.

(3) Ensuring that age assurance methods used by businesses that provide online services, products, or features likely to be accessed by children are proportionate to the risks that arise from the data management practices of the business, privacy protective, and minimally invasive.

(4) Assessing and mitigating risks to children that arise from the use of an online service, product, or feature.

(5) Publishing privacy information, policies, and standards in concise, clear language suited for the age of children likely to access an online service, product, or feature.

(6) How the working group and the Department of Justice may leverage the substantial and growing expertise of the California Privacy Protection Agency in the long-term development of data privacy policies that affect the privacy, rights, and safety of children online.

(e) On or before January 1, 2024, and every two years thereafter, the working group shall submit, pursuant to Section 9795 of the Government Code, a report to the Legislature regarding the recommendations described in subdivision (d).

(f) The members of the working group shall serve without compensation but shall be reimbursed for all necessary expenses actually incurred in the performance of their duties.

(g) This section shall remain in effect until January 1, 2030, and as of that date is repealed.

1798.99.33. (a) A business shall complete a Data Protection Impact Assessment on or before July 1, 2024, for any online service, product, or feature likely to be accessed by children offered to the public before July 1, 2024.

(b) This section does not apply to an online service, product, or feature that is not offered to the public on or after July 1, 2024.

1798.99.35. (a) Any business that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) per affected child for each negligent violation or not more than seven thousand five hundred dollars ($7,500) per affected child for each intentional violation, which shall be assessed and recovered only in a civil action brought in the name of the people of the State of California by the Attorney General.

(b) Any penalties, fees, and expenses recovered in an action brought under this title shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160,

with the intent that they be used to fully offset costs incurred by the Attorney General in connection with this title.

(c) (1) If a business is in substantial compliance with the requirements of paragraphs (1) through (4), inclusive, of subdivision (a) of Section 1798.99.31, the Attorney General shall provide written notice to the business, before initiating an action under this title, identifying the specific provisions of this title that the Attorney General alleges have been or are being violated.

(2) If, within 90 days of the notice required by this subdivision, the business cures any noticed violation and provides the Attorney General a written statement that the alleged violations have been cured, and sufficient measures have been taken to prevent future violations, the business shall not be liable for a civil penalty for any violation cured pursuant to this subdivision.

(d) Nothing in this title shall be interpreted to serve as the basis for a private right of action under this title or any other law.

(e) The Attorney General may solicit broad public participation and adopt regulations to clarify the requirements of this title.

1798.99.40. This title does not apply to the information or entities described in subdivision (c) of Section 1798.145.

SEC. 3. The Legislature finds and declares that this act furthers the purposes and intent of the California Privacy Rights Act of 2020.

SEC. 4. The Legislature finds and declares that Section 2 of this act, which adds Title 1.81.46 (commencing with Section 1798.99.28) to Part 4 of Division 3 of the Civil Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

The limitation is needed to encourage businesses, by protecting their proprietary interests, to mitigate risks to children online.

O

2021 California Assembly Bill No. 2273, California 2021-2022 Regular Session

CALIFORNIA BILL TEXT

TITLE: The California Age-Appropriate Design Code Act.

VERSION: Adopted
September 15, 2022
Wicks (A) , Cunningham (A) , Petrie-Norris (A), Allen (S) , Newman (S) , Stern (S)

Image 1 within document in PDF format.

SUMMARY: An act to add Title 1.81.47 (commencing with Section 1798.99.28) to Part 4 of Division 3 of, and to repeal Section 1798.99.32 of, the Civil Code, relating to consumer privacy.

TEXT:

Assembly Bill No. 2273

CHAPTER 320

An act to add Title 1.81.47 (commencing with Section 1798.99.28) to Part 4 of Division 3 of, and to repeal Section 1798.99.32 of, the Civil Code, relating to consumer privacy.

[Approved by Governor September 15, 2022. Filed with Secretary of State September 15, 2022.]

LEGISLATIVE COUNSEL'S DIGEST

AB 2273, Wicks. The California Age-Appropriate Design Code Act.

(1) Existing law, the California Privacy Rights Act of 2020, approved by the voters as Proposition 24 at the November 3, 2020, statewide general election, establishes the California Privacy Protection Agency. Existing law vests the agency with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018 and requires the agency to be governed by a board. Existing law requires businesses to protect consumer privacy and information, make certain disclosures to consumers regarding a consumer's rights under the act in a specified manner, and disclose to consumers that a consumer has the right to request specific pieces of information, including the categories of information those businesses have collected about that consumer.

Existing law, the Parent's Accountability and Child Protection Act, requires a person or business that conducts business in California and that seeks to sell specified products or services to take reasonable steps to ensure that the purchaser is of legal age at the time of purchase or delivery, including verifying the age of the purchaser. Existing law prohibits a person or business that is required to comply with these provisions from retaining, using, or disclosing any information it receives in an effort to verify age from a purchaser or recipient for any other purpose, except as specified, and subjects a business or person that violates these provisions to a civil penalty.

This bill would enact the California Age-Appropriate Design Code Act, which, commencing July 1, 2024, would, among other things, require a business that provides an online service, product, or feature likely to be accessed by children to comply with specified requirements, including a requirement to configure all default privacy settings offered by the online service, product, or feature to the settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children, and to provide privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service,

product, or feature. The bill would require a business, before any new online services, products, or features are offered to the public, to complete a Data Protection Impact Assessment, as defined, for any online service, product, or feature likely to be accessed by children and maintain documentation of this assessment as long as the online service, product, or feature is likely to be accessed by children. The bill would require a business to make a Data Protection Impact Assessment available, within 5 business days, to the Attorney General pursuant to a written request and would exempt a Data Protection Impact Assessment from public disclosure, as prescribed. The bill would prohibit a business that provides an online service, product, or feature likely to be accessed by children from taking proscribed action, including, if the end user is a child, using personal information for any reason other than a reason for which the personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children.

This bill would create the California Children's Data Protection Working Group to deliver a report to the Legislature regarding best practices for the implementation of these provisions, as specified. The bill would require the members of the working group to have certain expertise, including in the areas of children's data privacy and children's rights. The bill would require the working group to take input from a broad range of stakeholders, including from academia, consumer advocacy groups, and small, medium, and large businesses affected by data privacy policies, and make prescribed recommendations on best practices, including identifying online services, products, or features likely to be accessed by children.

This bill would authorize the Attorney General to seek an injunction or civil penalty against any business that violates its provisions. The bill would hold violators liable for a civil penalty of not more than $2,500 per affected child for each negligent violation or not more than $7,500 per affected child for each intentional violation. The bill would require any penalties, fees, and expenses recovered in an action brought under the act to be deposited in the Consumer Privacy Fund with the intent that they be used to fully offset costs incurred by the Attorney General in connection with the act.

(2) The California Privacy Rights Act of 2020 authorizes the Legislature to amend the act to further the purposes and intent of the act by a majority vote of both houses of the Legislature, as specified.

This bill would declare that its provisions further the purposes and intent of the California Privacy Rights Act of 2020.

(3) Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.

This bill would make legislative findings to that effect.

The people of the State of California do enact as follows:

SECTION 1. (a) The Legislature hereby finds and declares all of the following:

(1) The United Nations Convention on the Rights of the Child recognizes that children need special safeguards and care in all aspects of their lives.

(2) As children spend more of their time interacting with the online world, the impact of the design of online products and services on children's well-being has become a focus of significant concern.

(3) There is bipartisan agreement at the international level, in both the United States and in the State of California, that more needs to be done to create a safer online space for children to learn, explore, and play.

(4) Lawmakers around the globe have taken steps to enhance privacy protections for children on the understanding that, in relation to data protection, greater privacy necessarily means greater security and well-being.

(5) Children should be afforded protections not only by online products and services specifically directed at them, but by all online products and services they are likely to access. In order to help support the design of online products, services, and features, businesses should take into account the unique needs of different age ranges, including the following developmental stages: 0 to 5 years of age or "preliterate and early literacy"; 6 to 9 years of age or "core primary school years"; 10 to 12 years of age or "transition years"; 13 to 15 years of age or "early teens"; and 16 to 17 years of age or "approaching adulthood."

(6) In 2019, 81 percent of voters said they wanted to prohibit companies from collecting personal information about children without parental consent, and a 2018 poll of Californian parents and teens found that only 36 percent of teenagers and 32 percent of parents say that social networking internet websites do a good job explaining what they do with users' data.

(7) While it is clear that the same data protection regime may not be appropriate for children of all ages, children of all ages should nonetheless be afforded privacy and protection, and online products and services should adopt data protection regimes appropriate for children of the ages likely to access those products and services.

(8) Online services, products, or features that are likely to be accessed by children should offer strong privacy protections by design and by default, including by disabling features that profile children using their previous behavior, browsing history, or assumptions of their similarity to other children, to offer detrimental material.

(9) Ensuring robust privacy protections for children by design is consistent with the intent of the Legislature in passing the California Consumer Privacy Act of 2018, and with the intent of the people of the State of California in passing the California Privacy Rights Act of 2020, which finds and declares that children are particularly vulnerable from a negotiating perspective with respect to their privacy rights.

(10) The California Privacy Protection Agency, created by the California Privacy Rights Act of 2020, has substantial and growing expertise that is integral to the development of privacy policy in California.

(b) Therefore, it is the intent of the Legislature to promote privacy protections for children pursuant to the California Age-Appropriate Design Code Act.

(c) It is the intent of the Legislature that the California Age-Appropriate Design Code promote innovation by businesses whose online products, services, or features are likely to be accessed by children by ensuring that those online products, services, or features are designed in a manner that recognizes the distinct needs of children at different age ranges.

(d) It is the intent of the Legislature that businesses covered by the California Age-Appropriate Design Code may look to guidance and innovation in response to the Age-Appropriate Design Code established in the United Kingdom when developing online services, products, or features likely to be accessed by children.

(e) It is the intent of the Legislature that the California Children's Data Protection Working Group consider the guidance provided by the Information Commissioner's Office in the United Kingdom when developing and reviewing best practices or other recommendations related to the California Age-Appropriate Design Code.

(f) It is the intent of the Legislature that the California Children's Data Protection Working Group and the Department of Justice leverage the substantial and growing expertise of the California Privacy Protection Agency in the implementation of this title.

SEC. 2. Title 1.81.47 (commencing with Section 1798.99.28) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.47. THE CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT

1798.99.28. This title shall be known, and may be cited, as the California Age-Appropriate Design Code Act.

1798.99.29. The Legislature declares that children should be afforded protections not only by online products and services specifically directed at them but by all online products and services they are likely to access and makes the following findings:

(a) Businesses that develop and provide online services, products, or features that children are likely to access should consider the best interests of children when designing, developing, and providing that online service, product, or feature.

(b) If a conflict arises between commercial interests and the best interests of children, companies should prioritize the privacy, safety, and well-being of children over commercial interests.

1798.99.30. (a) For purposes of this title, the definitions in Section 1798.140 shall apply unless otherwise specified in this title.

(b) For the purposes of this title:

(1) "Child" or "children," unless otherwise specified, means a consumer or consumers who are under 18 years of age.

(2) "Data Protection Impact Assessment" means a systematic survey to assess and mitigate risks that arise from the data management practices of the business to children who are reasonably likely to access the online service, product, or feature at issue that arises from the provision of that online service, product, or feature.

(3) "Default" means a preselected option adopted by the business for the online service, product, or feature.

(4) "Likely to be accessed by children" means it is reasonable to expect, based on the following indicators, that the online service, product, or feature would be accessed by children:

(A) The online service, product, or feature is directed to children as defined by the Children's Online Privacy Protection Act (15 U.S.C. Sec. 6501 et seq.).

(B) The online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children.

(C) An online service, product, or feature with advertisements marketed to children.

(D) An online service, product, or feature that is substantially similar or the same as an online service, product, or feature subject to subparagraph (B).

(E) An online service, product, or feature that has design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children.

(F) A significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.

(5) "Online service, product, or feature" does not mean any of the following:

(A) A broadband internet access service, as defined in Section 3100.

(B) A telecommunications service, as defined in Section 153 of Title 47 of the United States Code.

(C) The delivery or use of a physical product.

(6) "Profiling" means any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

1798.99.31. (a) A business that provides an online service, product, or feature likely to be accessed by children shall take all of the following actions:

(1) (A) Before any new online services, products, or features are offered to the public, complete a Data Protection Impact Assessment for any online service, product, or feature likely to be accessed by children and maintain documentation of this assessment as long as the online service, product, or feature is likely to be accessed by children. A business shall biennially review all Data Protection Impact Assessments.

(B) The Data Protection Impact Assessment required by this paragraph shall 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. The Data Protection Impact Assessment shall address, to the extent applicable, all of the following:

(i) 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.

(ii) Whether the design of the online product, service, or feature could lead to children experiencing or being targeted by harmful, or potentially harmful, contacts on the online product, service, or feature.

(iii) Whether the design of the online product, service, or feature could permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct on the online product, service, or feature.

(iv) Whether the design of the online product, service, or feature could allow children to be party to or exploited by a harmful, or potentially harmful, contact on the online product, service, or feature.

(v) Whether algorithms used by the online product, service, or feature could harm children.

(vi) Whether targeted advertising systems used by the online product, service, or feature could harm children.

(vii) Whether and how the online product, service, or feature uses system design features to increase, sustain, or extend use of the online product, service, or feature by children, including the automatic playing of media, rewards for time spent, and notifications.

(viii) Whether, how, and for what purpose the online product, service, or feature collects or processes sensitive personal information of children.

(2) Document any risk of material detriment to children that arises from the data management practices of the business identified in the Data Protection Impact Assessment required by paragraph (1) and create a timed plan to mitigate or eliminate the risk before the online service, product, or feature is accessed by children.

(3) Within three business days of a written request by the Attorney General, provide to the Attorney General a list of all Data Protection Impact Assessments the business has completed.

(4) (A) For any Data Protection Impact Assessment completed pursuant to paragraph (1), make the Data Protection Impact Assessment available, within five business days, to the Attorney General pursuant to a written request.

(B) Notwithstanding any other law, a Data Protection Impact Assessment is protected as confidential and shall be exempt from public disclosure, including under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code).

(C) To the extent any information contained in a Data Protection Impact Assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, disclosure pursuant to this paragraph shall not constitute a waiver of that privilege or protection.

(5) Estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers.

(6) Configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.

(7) Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature.

(8) If the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, provide an obvious signal to the child when the child is being monitored or tracked.

(9) Enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.

(10) Provide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns.

(b) A business that provides an online service, product, or feature likely to be accessed by children shall not take any of the following actions:

(1) Use the personal information of any child in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child.

(2) Profile a child by default unless both of the following criteria are met:

(A) The business can demonstrate it has appropriate safeguards in place to protect children.

(B) Either of the following is true:

(i) Profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged.

(ii) The business can demonstrate a compelling reason that profiling is in the best interests of children.

(3) Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, or as described in paragraphs (1) to (4), inclusive, of subdivision (a) of

Section 1798.145, unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of children likely to access the online service, product, or feature.

(4) If the end user is a child, use personal information for any reason other than a reason for which that personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children.

(5) Collect, sell, or share any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary for the business to provide the service, product, or feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature.

(6) Collect any precise geolocation information of a child without providing an obvious sign to the child for the duration of that collection that precise geolocation information is being collected.

(7) Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being.

(8) Use any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age. Age assurance shall be proportionate to the risks and data practice of an online service, product, or feature.

(c) (1) A Data Protection Impact Assessment conducted by a business for the purpose of compliance with any other law complies with this section if the Data Protection Impact Assessment meets the requirements of this title.

(2) A single data protection impact assessment may contain multiple similar processing operations that present similar risks only if each relevant online service, product, or feature is addressed.

(d) This section shall become operative on July 1, 2024.

1798.99.32. (a) The California Children's Data Protection Working Group is hereby created to deliver a report to the Legislature, pursuant to subdivision (e), regarding best practices for the implementation of this title.

(b) Working Group members shall consist of Californians with expertise in at least two of the following areas:

(1) Children's data privacy.

(2) Physical health.

(3) Mental health and well-being.

(4) Computer science.

(5) Children's rights.

(c) The working group shall select a chair and a vice chair from among its members and shall consist of the following 10 members:

(1) Two appointees by the Governor.

(2) Two appointees by the President Pro Tempore of the Senate.

(3) Two appointees by the Speaker of the Assembly.

(4) Two appointees by the Attorney General.

(5) Two appointees by the California Privacy Protection Agency.

(d) The working group shall take input from a broad range of stakeholders, including from academia, consumer advocacy groups, and small, medium, and large businesses affected by data privacy policies and shall make recommendations to the Legislature on best practices regarding, at minimum, all of the following:

(1) Identifying online services, products, or features likely to be accessed by children.

(2) Evaluating and prioritizing the best interests of children with respect to their privacy, physical health, and mental health and well-being and evaluating how those interests may be furthered by the design, development, and implementation of an online service, product, or feature.

(3) Ensuring that age assurance methods used by businesses that provide online services, products, or features likely to be accessed by children are proportionate to the risks that arise from the data management practices of the business, privacy protective, and minimally invasive.

(4) Assessing and mitigating risks to children that arise from the use of an online service, product, or feature.

(5) Publishing privacy information, policies, and standards in concise, clear language suited for the age of children likely to access an online service, product, or feature.

(6) How the working group and the Department of Justice may leverage the substantial and growing expertise of the California Privacy Protection Agency in the long-term development of data privacy policies that affect the privacy, rights, and safety of children online.

(e) On or before January 1, 2024, and every two years thereafter, the working group shall submit, pursuant to Section 9795 of the Government Code, a report to the Legislature regarding the recommendations described in subdivision (d).

(f) The members of the working group shall serve without compensation but shall be reimbursed for all necessary expenses actually incurred in the performance of their duties.

(g) This section shall remain in effect until January 1, 2030, and as of that date is repealed.

1798.99.33. (a) A business shall complete a Data Protection Impact Assessment on or before July 1, 2024, for any online service, product, or feature likely to be accessed by children offered to the public before July 1, 2024.

(b) This section does not apply to an online service, product, or feature that is not offered to the public on or after July 1, 2024.

1798.99.35. (a) Any business that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) per affected child for each negligent violation or not more than seven thousand five hundred dollars ($7,500) per affected child for each intentional violation, which shall be assessed and recovered only in a civil action brought in the name of the people of the State of California by the Attorney General.

(b) Any penalties, fees, and expenses recovered in an action brought under this title shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160, with the intent that they be used to fully offset costs incurred by the Attorney General in connection with this title.

(c) (1) If a business is in substantial compliance with the requirements of paragraphs (1) through (4), inclusive, of subdivision (a) of Section 1798.99.31, the Attorney General shall provide written notice to the business, before initiating an action under this title, identifying the specific provisions of this title that the Attorney General alleges have been or are being violated.

(2) If, within 90 days of the notice required by this subdivision, the business cures any noticed violation and provides the Attorney General a written statement that the alleged violations have been cured, and sufficient measures have been taken to prevent future violations, the business shall not be liable for a civil penalty for any violation cured pursuant to this subdivision.

(d) Nothing in this title shall be interpreted to serve as the basis for a private right of action under this title or any other law.

(e) The Attorney General may solicit broad public participation and adopt regulations to clarify the requirements of this title.

1798.99.40. This title does not apply to the information or entities described in subdivision (c) of Section 1798.145.

SEC. 3. The Legislature finds and declares that this act furthers the purposes and intent of the California Privacy Rights Act of 2020.

SEC. 4. The Legislature finds and declares that Section 2 of this act, which adds Title 1.81.46 (commencing with Section 1798.99.28) to Part 4 of Division 3 of the Civil Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

The limitation is needed to encourage businesses, by protecting their proprietary interests, to mitigate risks to children online.

West's Annotated California Codes
Civil Code (Refs & Annos)
Division 3. Obligations (Refs & Annos)
Part 4. Obligations Arising from Particular Transactions (Refs & Annos)
Title 1.81.5. California Consumer Privacy Act of 2018 (Refs & Annos)

West's Ann.Cal.Civ.Code § 1798.140

§ 1798.140. Definitions [1]

Effective: January 1, 2023
Currentness

For purposes of this title:

(a) "Advertising and marketing" means a communication by a business or a person acting on the business' behalf in any medium intended to induce a consumer to obtain goods, services, or employment.

(b) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(c) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(d) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households.

(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers' personal information. “Control” or “controlled” means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. “Common branding” means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

(4) A person that does business in California, that is not covered by paragraph (1), (2), or (3), and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

(e) “Business purpose” means the use of personal information for the business' operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (11) of subdivision (a) of Section 1798.185, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.

(5) Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.

(7) Undertaking internal research for technological development and demonstration.

(8) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(f) “Collects,” “collected,” or “collection” means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(g) “Commercial purposes” means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

(h) “Consent” means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

(i) “Consumer” means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(j)(1) “Contractor” means a person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract with the business, provided that the contract:

(A) Prohibits the contractor from:

(i) Selling or sharing the personal information.

(ii) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.

(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and the business.

(iv) Combining the personal information that the contractor receives pursuant to a written contract with the business with personal information that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the contractor may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) and in regulations adopted by the California Privacy Protection Agency.

(B) Includes a certification made by the contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.

(C) Permits, subject to agreement with the contractor, the business to monitor the contractor's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(k) “Cross-context behavioral advertising” means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

(*l*) “Dark pattern” means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.

(m) “Deidentified” means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:

(1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.

(2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.

(3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision.

(n) “Designated methods for submitting requests” means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(*o*) “Device” means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(p) “Homepage” means the introductory page of an internet website and any internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, “About,” “Information," or settings page, and any other location that allows consumers to review the notices required by this title, including, but not limited to, before downloading the application.

(q) “Household” means a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common devices or services.

(r) “Infer” or “inference” means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(s) “Intentionally interacts” means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, including visiting the person's website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.

(t) “Nonpersonalized advertising” means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business with the exception of the consumer's precise geolocation.

(u) “Person” means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(v)(1) “Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(L) Sensitive personal information.

(2) “Personal information” does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, “publicly available” means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) “Personal information” does not include consumer information that is deidentified or aggregate consumer information.

(w) "Precise geolocation" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations.

(x) "Probabilistic identifier" means the identification of a consumer or a consumer's device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(y) "Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(z) "Profiling" means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(aa) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(ab) "Research" means scientific analysis, systematic study, and observation, including basic research or applied research that is designed to develop or contribute to public or scientific knowledge and that adheres or otherwise conforms to all other applicable ethics and privacy laws, including, but not limited to, studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, by a business.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, other than as needed to support the research.

(4) Subject to business processes that specifically prohibit reidentification of the information, other than as needed to support the research.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals as are necessary to carry out the research purpose.

(ac) “Security and integrity” means the ability of:

(1) Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.

(2) Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.

(3) Businesses to ensure the physical safety of natural persons.

(ad)(1) “Sell,” “selling,” “sale,” or “sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally:

(i) Disclose personal information.

(ii) Interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a

business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ae) "Sensitive personal information" means:

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(2)(A) The processing of biometric information for the purpose of uniquely identifying a consumer.

(B) Personal information collected and analyzed concerning a consumer's health.

(C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

(3) Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information.

(af) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(ag)(1) "Service provider" means a person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from:

(A) Selling or sharing the personal information.

(B) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title.

(C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.

(D) Combining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(ah)(1) “Share,” “shared,” or “sharing” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

(2) For purposes of this title, a business does not share personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information

of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ai) "Third party" means a person who is not any of the following:

(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under this title.

(2) A service provider to the business.

(3) A contractor.

(aj) "Unique identifier" or "unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.

(ak) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can verify, using commercially reasonable methods, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115, to delete personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

Credits

(Added by Stats.2018, c. 55 (A.B.375), § 3, eff. Jan. 1, 2019, operative Jan. 1, 2020. Amended by Stats.2018, c. 735 (S.B.1121), § 9, eff. Sept. 23, 2018, operative Jan. 1, 2020; Stats.2019, c. 748 (A.B.874), § 1, eff. Jan. 1, 2020; Stats.2019, c. 757 (A.B.1355), § 7.5, eff. Jan. 1, 2020; Initiative Measure (Prop. 24, § 14, approved Nov. 3, 2020, eff. Dec. 16, 2020, operative Jan. 1, 2023); Stats.2021, c. 525 (A.B.694), § 3, eff. Jan. 1, 2022, operative Jan. 1, 2023.)

Editors' Notes

OPERATIVE EFFECT

<For effective and operative dates of Initiative Measure (Prop. 24), see § 31 of the Measure.>

<For operative effect of Title 1.81.5, see Civil Code § 1798.198.>

Notes of Decisions (1)

Footnotes

1 Section caption supplied by Prop. 24.

West's Ann. Cal. Civ. Code § 1798.140, CA CIVIL § 1798.140
Current with all laws through Ch. 997 of 2022 Reg.Sess.

End of Document

United States Code Annotated
Constitution of the United States
Annotated
Amendment I. Religion; Speech and the Press; Assembly; Petition

U.S.C.A. Const. Amend. I

Amendment I. Establishment of Religion; Free Exercise of Religion; Freedom of Speech and the Press; Peaceful Assembly; Petition for Redress of Grievances

Currentness

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

<Historical notes and references are included in the full text document for this amendment.>

<For Notes of Decisions, see separate documents for clauses of this amendment:>

<USCA Const Amend. I--Establishment clause; Free Exercise clause>

<USCA Const Amend. I--Free Speech clause; Free Press clause>

<USCA Const Amend. I--Assembly clause; Petition clause>

U.S.C.A. Const. Amend. I, USCA CONST Amend. I
Current through P.L. 118-22. Some statute sections may be more current, see credits for details.

End of Document

CERTIFICATE OF SERVICE

Case Name: **NetChoice, LLC v Rob Bonta** No. **23-2969 [Appeal]**

I hereby certify that on December 13, 2023, I electronically filed the following documents with the Clerk of the Court by using the CM/ECF system:

ADDENDUM

Participants in the case who are registered CM/ECF users will be served by the CM/ECF system.

I am employed in the Office of the Attorney General, which is the office of a member of the California State Bar at which member's direction this service is made. I am 18 years of age or older and not a party to this matter. I am familiar with the business practice at the Office of the Attorney General for collection and processing of correspondence for mailing with the United States Postal Service. In accordance with that practice, correspondence placed in the internal mail collection system at the Office of the Attorney General is deposited with the United States Postal Service with postage thereon fully prepaid that same day in the ordinary course of business.

I further certify that some of the participants in the case are not registered CM/ECF users. On December 13, 2023, I have caused to be mailed in the Office of the Attorney General's internal mail system, the foregoing document(s) by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within three (3) calendar days to the following non-CM/ECF participants:

District Judge Beth Labson Freeman
San Jose Courthouse, Courtroom 3 – 5th Floor
280 South 1st Street
San Jose, CA 95113

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 and that this declaration was executed on December 13, 2023, at Los Angeles, California.

J. Sissov	/s/ *J. Sissov*
Declarant	Signature

SA2023305531