Alan Butler (SBN 281291)
butler@epic.org
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue NW
Washington, DC 20036
Tel: 202.483.1140

Meetali Jain (SBN 214237)
meetali@reset.tech
RESET TECH
1200 17th St NW, Suite 501
Washington, DC 20036

Attorneys for Proposed Amicus Curiae Electronic Privacy Information Center, Reset Tech, Frances Haugen, and Former Government Officials

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

NETCHOICE, LLC, d/b/a NetChoice,

Plaintiff,

v.

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

Defendant.

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

BRIEF OF ELECTRONIC PRIVACY INFORMATION CENTER, RESET TECH, FRANCES HAUGEN, AND FORMER GOVERNMENT OFFICIALS FOR LEAVE TO SUBMIT BRIEF AS *AMICI CURIAE* IN SUPPORT OF DEFENDANT

Hearing Date: July 27, 2023
Time: 1:30 p.m.
Judge: Hon. Beth Labson Freeman
Court: Courtroom 1, 5th Floor

Action Filed: December 14, 2022

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES & REGULATIONS

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*[1]

EPIC is a nonpartisan, nonprofit organization established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC's mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.

Reset Tech aims to reset the connection between media and democracy by countering the threats posed by digital media monopolies. Reset develops and promotes new ideas to change policy, engages with governments, supports public campaigns, and funds research to promote change and offer solutions.

EPIC and Reset are joined on this brief by Frances Haugen, Facebook whistleblower and tech expert, as well as a bipartisan group of former elected and appointed officials at both federal and state level, including several from the State of California, united by a commitment to find workable legislative solutions to the digital harms faced by children and young people today. This bipartisan group of amici includes:

Hannah-Beth Jackson (CA)
- Former California State Senator and Chair of Senate Judiciary Committee.

Jordan Cunningham (CA)
- Former California Assembly member and joint-author of California Age Appropriate Design Code Act.

William "Bill" Monning (CA)
- Former California State Senator.

Bob Wieckowski (CA)
- Former California State Senator and Assembly Judiciary Committee chair and member.

Dick Gephardt (US)
- Former US Representative for Missouri.

[1] *Amici* certify that no person or entity, other than *Amici*'s own staff or counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief, in whole or in part.

Kerry Healey (MA)
- Former Lieutenant Governor of the Commonwealth of Massachusetts.

Steve Israel (US)
- Former US Representative from New York and the Director of the nonpartisan Institute of Politics and Global Affairs at Cornell University.

Cheri Bustos (US)
- Former US Representative from Illinois.

Dan Glickman (US)
- Former US Secretary of Agriculture, former US Representative from Kansas, and former director of the Institute of Politics at Harvard University's John F. Kennedy School of Government.

Chris Shays (US)
- Former US Representative from Connecticut.

Linda Douglass (US)
- Former Head of Communications for Bloomberg, Senior Vice President at Atlantic Media and former Communications Director in the White House's Office of Health Reform.

Admiral Bill Owens
- Former Vice Chairman of the Joint Chiefs of Staff and U.S. Navy Admiral.

Amici believe the framework offered by the California Age Appropriate Design Code (AADC), specifically addressing the risks to children that arise from the data management practices of online services, including social media, is a sensible and effective means of confronting tech's harmful business model. *Amici* have decades of experience evaluating state and federal legislative proposals and considering the limits imposed on state law by federal preemption and the Constitution, and *amici* believe the AADC's approach to tech regulation is consistent with Section 230 and the First Amendment. Their ultimate interest here is ensuring that the Court's judgment about the AADC is based on a wholistic understanding of how the statute fits into the broader landscape of privacy and technology regulation.

INTRODUCTION

The California Age-Appropriate Design Code ("AADC") is a landmark piece of legislation enacted to require platforms to design their services with children's privacy in mind. The law imposes certain obligations on companies that use children's personal information to profile and target them. The law does not require companies to remove or even demote any specific content—as long as they do not use children's data in a way that violates the law, companies can show users whatever information they like.

Amici offer their particular expertise to counter two of the arguments Plaintiff and their *amici* aim at the AADC. First, Section 230 of the Communications Decency Act does not preempt or otherwise bar the law. Section 230 protects companies from publisher liability for content third parties post to their platforms. It does not immunize companies from suits alleging harms traceable to their own conduct. Here, because the AADC regulates platforms' own conduct—specifically, how platforms use children's personal information—Section 230 simply does not apply. How companies use personal information is the type of conduct that privacy laws commonly regulate. Section 230 should not be read so broadly as to undermine privacy regulation generally. Moreover, even if Section 230 provided immunity from suits under the AADC, it can only be used as a defense to liability, not as a preemptive facial attack, as Plaintiff attempt here.

Second, and relatedly, the data protection and privacy requirements in the AADC do not effect an unlawful prior restraint. To the contrary, the impact assessments required by the AADC are common in regulatory frameworks across the United States and the world, and numerous laws incorporate similar requirements. Indeed, large online platforms and services already undertake data protection assessments, which promote consumer trust. The argument that generally applicable privacy regulations, targeted specifically at mitigating harms to children's privacy, are unconstitutional would undermine numerous federal and state laws and undermine the state's compelling interest in protecting the privacy of children.

ARGUMENT

I. Section 230 of the Communications Decency Act does not preempt California's ability to regulate how platforms use children's data, and as a matter of procedure that argument should not be considered on this posture.

Congress passed Section 230 of the Communications Decency Act to protect companies from liability for the content third parties publish on their platforms. In the years since, however, internet companies have repeatedly invoked Section 230 immunity not only in suits involving publisher liability, but also in suits targeting platforms' own conduct. Over the last twenty-five plus years, appellate courts have increasingly rejected such arguments. This Court should similarly reject Plaintiff's invocation of Section 230 for two reasons: first, Section 230 does not preempt the AADC because it explicitly regulates platforms' own conduct, not any third-party content. And second, Plaintiff invokes Section 230 at the wrong time—it provides a defense from liability, not an opportunity for a preemptive facial attack. For either reason, this Court should reject Plaintiff's Section 230 arguments.

A. Section 230 does not immunize platforms in suits about their own conduct.

Plaintiff's Complaint and Motion for Preliminary Injunction invoke the protections of Section 230 without acknowledging key limits to the statute's application. Section 230 immunizes platforms from publisher liability for third-party content. However, when lawsuits concern harms allegedly caused by platforms' own conduct, Section 230 does not provide immunity. Conduct that includes platforms' own design choices—such as what data to collect, and how to use that data in designing products—falls outside of the scope of the statute. Courts of Appeals, including the Ninth Circuit, have long distinguished between liability for third-party content and platform conduct under Section 230 in cases addressing possible platform violations of federal, state, and local laws, including anti-discrimination laws, consumer protection laws, and other statutes and ordinances. Indeed, platforms themselves have begun to acknowledge

this, including most recently Plaintiff NetChoice's member Google at the oral argument in *Gonzalez v. Google*, currently pending at the Supreme Court.

Courts of Appeals have consistently refused to extend Section 230 to shield platforms from liability for their own intentional conduct. Recently, this Court and the Ninth Circuit have rejected Section 230 immunity when invoked by platforms in suits addressing the business practices of the platforms. In *Airbnb, Inc. v. City & County of San Francisco*, 217 F. Supp. 3d 1066, 1073 (N.D. Cal. 2016), this Court held that an online vacation rental platform could face liability for violating local ordinances prohibiting unlicensed vacation rentals. The Ninth Circuit later reached the same result in a similar case. *See HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 683 (9th Cir. 2019). In both of those cases, platform defendants could not invoke Section 230 immunity because the platforms' alleged conduct that violated the ordinance was not tied to any specific third party-content—the rental listings themselves—at all. The platforms had made decisions about where, how, and to whom to offer listings in ways that violated local law. "[T]he vacation rental platforms did not face liability for the content of their listings; rather liability arose from facilitating unlicensed booking transactions." *Dyroff v. Ultimate Software Group, Inc.*, 934 F.3d 1093, 1098 (9th Cir. 2019) (discussing and characterizing *HomeAway.com*). Put more generally, if a platform could modify its own conduct—its data practices, its design of a recommender algorithm, its user features—to comply with applicable law without reference to any specific piece of third-party content, the illegality comes from the platform's choices, and Section 230 immunity does not apply.

Cases involving alleged violations of anti-discrimination law are particularly relevant applications of this rule. In one such case, the Ninth Circuit held that a platform could not invoke Section 230 immunity to defend against claims it had violated anti-discrimination law when it specifically solicited racial preferences from users seeking roommates. Designing a feature that uses personal information about users—such as their race or gender—to decide whether to show them housing ads is "something the law prohibits" in its own right. *Fair Housing Council v. Roommates.com*, 521 F.3d 1157, 1167 (9th Cir. 2008) (en banc). Federal

agencies agree that platforms that use information about a person's membership in a protected class to target ads in violation of anti-discrimination law do not enjoy Section 230 immunity. *See, e.g.*, *HUD. v. Facebook*, Charge of Discrimination, FHEO No. 01-18-0323-8 at 4. Platforms themselves have even begun to acknowledge that such conduct is not covered by Section 230. When asked whether Section 230 gives platforms immunity from anti-discrimination laws, counsel for one of Plaintiff's own members, Google, recently admitted that targeting information to users based on their race "has nothing to do with the content of third-party information." *Oral argument transcript* at 128, *Gonzalez v. Google*, No. 21-1333 (U.S.), *pending*. Like anti-discrimination laws, the AADC regulates how companies target information to kids based on their personal information. It does not impose liability for third-party content itself.

The Ninth Circuit has also rejected Section 230 immunity for a platform defendant whose design choices caused harm to young people. In *Lemmon v. Snap*, 995 F.3d 1085 (9th Cir. 2021), plaintiffs had alleged harm from "an incentive system within Snapchat that encouraged its users to . . . drive at speeds exceeding 100 MPH." *Id.* at 1092–92. While the platform strenuously asserted Section 230 immunity, arguing that plaintiffs sought to hold it responsible for content ultimately created and posted by third-party users, the Court rejected that. *Id*. at 1094. If a plaintiff's claim turns on whether the platform should be treated as a publisher of third-party content, or whether they improperly removed third-party content, the platform can get immunity—but that's not what the *Lemmon* complaint alleged. The complaint alleged a legally-cognizable injury caused by negligent design of the incentive system in the platform itself. And when lawsuits allege harms caused by platforms' own negligent design choices, a platform cannot invoke Section 230 liability. *Id*. at 1091–94; *see also Erie Ins. Co. v. Amazon.com, Inc.*, 925 F.3d 135 (4th Cir. 2019) (declining to apply Section 230 immunity in suit about sale of defective goods, even though marketing copy ultimately came from third-party sellers on the Amazon platform).

B. Section 230 does not preempt the AADC because it regulates how platforms use children's data to design their services and imposes no liability for publishing third-party content.

The AADC does not treat platforms as publishers of third-party content. Like suits the Ninth Circuit addressed in cases like *HomeAway*, *Roommates.com*, and *Lemmon*, the AADC regulates business conduct—specifically, how companies design their services using children's data.

The text of the law makes this clear. The AADC applies to platforms "when designing, developing, and providing [an] online service, product or feature." Cal. Civ. Code § 1798.99.29(a). The statute specifically calls on platforms to evaluate "how [they use] children's personal information, and the risks of material detriment to children that arise from the data management practices of the business," *id.* § 1798.99.31(a)(1)(B), and refers to platform design in many ways including the "design elements," § 1798.99.30(b)(4)(E), "the design of the online product," § 1798.99.31(a)(1)(B)(i)-(iv), "algorithms used by the online product," § 1798.99.31 (a)(1)(B)(v), and "system design features," § 1798.99.31 (a)(1)(B)(vii). The prescriptive sections of the AADC reflect this too, focusing on platform design choices fully within platform control and far from the heartland of Section 230 immunity. *See* §§ 1798.99.31(a)(2) (requiring companies to create plans to mitigate risks created by their use of children's personal information); 1798.99.31(a)(3)–(4) (requiring certain disclosures to the Attorney General); 1798.99.31(a)(5) (requiring companies to estimate the age of child users); 1798.99.31(a)(6) (setting requirements for default privacy settings); 1798.99.31(a)(7) (requiring disclosure of privacy information); 1798.99.31(a)(8) (requiring companies inform children if they are being tracked by parents); 1798.99.31(a)(9) (calling for enforcement of platform's own terms); 1798.99.31(a)(10) (requiring a contact tool); 1798.99.31(b)(i)–(ii) (prohibiting other platform data practices).

A platform would not have to remove or even demote any content to comply with these requirements. Platforms could show users whatever content they like—as long as the companies ensure that that they are not using children's data to target information to them in violation of

the law. Indeed, a company that does not use kids' data to target content cannot violate the key provisions of the law regardless of whether the content could cause harm to kids. Thus, like the examples discussed in the previous section, the AADC does not impose liability for third-party content—it holds platforms liable for their own conduct.

The purposes of the AADC further show that the law imposes liability based on platform conduct—how a platform uses kids' data to target information—and not on what content the platform shows children. The AADC, like many business regulations across economic sectors, seeks to address market incentives that the legislature believes currently encourage businesses to design and produce harmful products. *See id.* § 1798.99.29(b) (discussing "conflict . . . between commercial interests and the best interests of children"). California's motivation to enact the AADC tracks with governments' motivation to regulate businesses' *conduct* across economic sectors. Many business regulations address negative externalities, or situations where businesses make money but cause harm to or impose costs on communities or the public while doing so. And as the statute notes here, online platforms react to business incentives in ways that undermine privacy rights. *See* Findings Section at (b)–(d). Platforms have built-in profit incentives to optimize their internal platform designs not to protect privacy—of children or adults—but to promote engagement. *See, e.g.*, Gilad Edelman, *How Facebook Could Break Free From the Engagement Trap*, Wired (Nov. 19, 2021), https://www.wired.com/story/jeff-allen-interview-facebook-engagement-trap/. This is because users who spend more time on a platform see more ads, which helps platforms make money. Understandably, under current incentives, platforms make design choices to prioritize content that prompts people to engage and spend more time on the platform. *See generally* Allen, Jeff, *Social Media and the Spread of Harmful Content*, Grand Rounds in the Oakland Department of Psychiatry, 22 June 2022, Oakland CA (virtual), https://static1.squarespace.com/static/614cbb3258c5c87026497577/t/6389125816e7a1745103a09c/1669927516632/Social+Media+and+the+Spread+of+Harmful+Content.pdf. And as the head of one of Plaintiff's members has previously explained, the closer content grows to violating

policies against incitement to violence, promotion of self-harm, or misinformation, the more users engage. *See* Mark Zuckerberg, *A Blueprint for Content Governance and Enforcement*, Facebook (last edited May 5, 2021), http://www.facebook.com/notes/751449002072082/. When this kind of content is targeted at a child based on information the company has collected about the child and inferences the company has made from that information, the harmful effect is especially acute. It is this specific harm that the AADC protects against.

Section 230 prohibits holding platforms liable for specific content posted by third parties. But Section 230 does not prevent California from regulating the incentives and business practices of the platforms, including platforms' incentive to use a child's personal data to entice them to stay on the platform. The Court should reject arguments that Section 230 preempts the AADC.

C. Even if Section 230 properly applied here, Plaintiff's invocation comes at an inappropriate time.

This Court should reject Plaintiff's proposed application of Section 230 for an entirely separate reason: it does not presently, and may never, face civil liability from which Section 230 provides immunity.

Section 230 protects platforms from a "cause of action" that "may be brought" under a state law that is "inconsistent" with the provision. 42 U.S.C. § 230(e)(3). Section 230 provides a defense to lawsuits; it does not provide the basis for facial challenges to statutes or regulations. Indeed, courts often hesitate to apply Section 230 immunity at even the pleading stage unless application of "the statute's barrier to suit is evident from the face of the complaint." *Marshall's Locksmith v. Google, LLC,* 925 F.3d 1263, 1267 (D.C. Cir. 2019).

Here, Plaintiff does not allege—nor could it—that any actions under the AADC are threatened or imminent, or even that they are likely to happen at all. While part of the AADC allows for the California Attorney General, alone, to seek civil penalties for certain violations, *see* Cal. Civil Code § 1798.99.35(a), any such suits cannot be brought as yet to any current online service, product, or feature. *See id.* § 1798.99.33(b). Plaintiff speculates not only that

Defendant will imminently bring such actions, but that such actions would apply the law in ways inconsistent with Section 230. None of those things are clear. Under the circumstances, this Court should decline to apply Section 230 at this juncture.

II. Data protection impact requirements do not effect an unlawful prior restraint on platforms.

This is a case about a privacy statute that applies tools commonly used in global data protection frameworks to address harmful business practices targeted at children. This is not a case about censorship or speech restrictions for similar reasons to why the AADC does not regulate third-party content. The focus of the statute is on the assessment and mitigation of risks caused by business' collection and use of children's personal data. Merely requiring a company to assess and mitigate the risks of harmful data processing is not an unconstitutional prior restraint. If the Court were to hold that the AADC framework violates the First Amendment, it could undermine a wide range of state and federal privacy laws and raise concerns about international data protection frameworks as well.

Companies have tried for decades to argue that privacy laws violate their First Amendment rights. But despite their efforts, courts have generally upheld privacy regulations at the state and federal level where they do not inhibit public discussions on matters of public concern. *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. Rev. 1149, 1155 (2005); Neil M. Richards, *Why Data Protection Law is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1505 (2015). Indeed, most privacy law provisions are common business regulations that should be subject to simple rational basis review and easily pass constitutional muster. *See* Richards, *Reconciling Data Privacy*, *supra*, at 117374. And courts have also gone further to uphold privacy statutes that directly limit the transfer, sale, and even collection of personal information; these statutes impose a much more direct burden on speech than the impact assessment requirements in the AADC. *See, e.g.*, *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (affirming FCC regulations applying privacy regulations concerning the collection of consumer proprietary network information under 47 U.S.C. § 222);

TransUnion v. FTC, 267 F.3d 1138, 1142 (D.C. Cir. 2001) (upholding the Fair Credit Reporting Act ban on target marketing lists). It is not surprising that many other state and federal privacy laws have stood for decades without a significant First Amendment challenge. *See, e.g.,* 47 U.S.C. § 551 (Cable Subscriber Privacy Provisions), 18 U.S.C. § 2710 (Video Privacy Protection Act), Cal. Penal Code § 630 (California Invasion of Privacy Act), 201 Code of Mass. Reg. 17.00. Even when evaluated under the stricter *Central Hudson* test, these laws "directly advance" the "substantial" governmental interest in protecting the privacy and security of personal information and thus clearly satisfy the standards set forth in *Central Hudson Gas Electric Corporation v. Public Service Commission of New York*, 447 U.S. 557 (1980). *See NCTA v. FCC*, 555 F.3d at 998; *see also Sorrell v. IMS Health Inc.*, 564 U.S. 552, 596 (2011) (Breyer, J., dissenting) (citing *DOJ v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 762–771 (1989)); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 520–22 (2006).

The AADC is on even stronger constitutional footing than other privacy laws that have been in force for decades. The law not only directly advances the government's substantial interest in protecting the privacy of personal information, but also directly advances the government's substantial interest in preventing or mitigating harms to children. And the impact assessments that the AADC requires are commonplace risk mitigation mechanisms that are already being used by large companies and are being integrated into major global privacy frameworks. Ruling that the AADC's impact assessment requirements violate the First Amendment would pose an existential threat to nearly all privacy regulations in the United States.

A. The AADC imposes data protection requirements specifically tailored to ensure businesses mitigate harmful data practices that impact children.

Most privacy and data protection laws require companies to conduct Data Protection Impact Assessments (DPIAs) on certain data processing activities, particularly if those activities may include large-scale, high-risk, or sensitive data processing. *See, e.g.,* Cal. Civ. Code §

1798.185(a)(15)(B); Col. Rev. Stat. § 6-1-1309(2)(a)-(c); European Union Regulation 2016/679 (General Data Protection Regulation) Art. 35; Brazil Lei Geral de Proteção de Dados (LGPD) Art. 38. These DPIAs are important tools used to evaluate data processing activities, typically including the scope and purpose of data processing and potential risks to the data subjects. *See, e.g.,* General Data Protection Regulation Article 35; Cal. Civ. Code §1798.185(a)(15)(B); Col. Rev. Stat. § 6-1-1309(2)(a)-(c). These assessments ultimately focus on commercial conduct, a business's policies and practices for collecting, using, storing, and transferring personal data, and not on traditionally expressive conduct.

The DPIAs required by the AADC are specifically tailored to assess "the purpose of the online service, product, or feature, how it uses children's personal information, and the risks of material detriment to children that arise from the data management practices of the business." Cal. Civ. Code § 1798.99.31(a)(1)(B). Additional items that the applicable business must address in the assessment include potential harms stemming from the design of the product, service, or feature, algorithms used in the product, service, or feature, targeted advertising systems used by the product, service, or feature, and sensitive data processing. Cal. Civ. Code § 1798.99.31(a)(1)(B)(i-viii). These requirements are not directed at specific speech or expressive conduct. The only mention of "content" in the statute is in the list of considerations for businesses conducting the assessments, and even there it is the design of the system that must be evaluated, not the content itself. Cal. Civ. Code § 1798.99.31(a)(1)(B)(i).

The AADC establishes an audit and assessment process that requires businesses to evaluate risks that their services and data collection systems could pose to children. The law sets forth what questions must be asked but does not presuppose the answers to those questions. And if a risk is revealed in the course of conducting the DPIA, the practice is not automatically prohibited—the business is tasked with creating a plan to mitigate or eliminate the risk generated by the processing activity. Cal. Civ. Code § 1798.99.31(a)(2). Again, this requirement does not mandate a specific action (or require "self-censorship") but encourages businesses to

improve the design of their processing activity to lessen risks to data subjects. *Id*. It is left up to the business how and to what extent the risk will be mitigated or eliminated.

Even the mitigation requirement of the AADC will only apply in a narrow range of cases where a business finds a "risk of material detriment to children that arises from the data management practices of the business identified in the Data Protection Impact Assessment." *Id*. Indeed, the only prohibitions in the statute are prohibitions on use, collection, or transfer of children's personal information. Cal. Civ. Code § 1798.99.31(b).

B. Data protection impact assessments are already commonplace for large online services and have long been integrated into global privacy frameworks and standards.

This challenge to the use of DPIAs does not occur in a vacuum. DPIAs are a routine and common data protection tool in privacy legislation both within the U.S. and globally. Several U.S. state laws require in-scope businesses to complete DPIAs for existing and new processing activities. *See, e.g.,* Cal. Civ. Code § 1798.185(a)(15)(B); Va. Code Ann. § 59.1-576(A)(1-5); Col. Rev. Stat. § 6-1-1309(2)(a)-(c); Conn. Gen. Stat. Chapter 743jj § 42-552. Internationally, privacy and data security laws frequently mandate regular DPIAs. *See, e.g.*, General Data Protection Regulation Art. 35; United Kingdom General Data Protection Regulation Art. 35; Brazil LGPD Art. 38; Abu Dhabi Global Market Data Protection Regulations 2021 Section 34; Mauritius Data Protection Act 2017 Section 34; South Africa Protection of Personal Information Act Section 4(b).

As recognized by many of these regulations and accompanying guidance, DPIAs are essential privacy tools that aid the applicable business in demonstrating compliance with legal obligations, assessing data collection and processing practices, and identifying risks. *See, e.g.,* United Kingdom Information Commissioner's Office Data Protection Impact Assessments Guidance; General Data Protection Regulation Art. 35 and Recital 90. By requiring businesses to carefully evaluate the structure, necessity, and impact of a processing activity prior to deployment, DPIAs put into action key privacy principles, including accountability, data minimization, and privacy by design. *See* United Kingdom Information Commissioner's Office

Data Protection Impact Assessments Guidance. Consistent DPIA use trains staff involved in designing projects to consider privacy in early stages, which both produces better privacy outcomes and prevents the business from wasting time and resources on shutting down or fixing ill-considered, harmful, or non-compliant practices after they are already in use.

These assessments are also critical tools for both enforcement bodies and businesses in enforcement proceedings. Enforcement authorities often review DPIAs as part of an enforcement investigation, particularly as a method of confirming whether businesses have made appropriate effort to comply with applicable regulations. On the business side, DPIAs allow businesses to "show their work" and prove to authorities that businesses are aware of their privacy obligations and carefully considering them in every stage of service, product, or feature development.

A business can also publish the assessments to promote consumer trust. In the event that a problem arises, businesses can point to DPIAs to demonstrate that they have carefully considered consumer interests and attempted to reduce or remove negative impacts as much as possible. DPIAs also may allow consumers to better understand how and why their information is being used.

DPIAs are a key privacy compliance and assessment tool internationally and an integral component of many privacy compliance and enforcement regimes. Invalidating this tool poses a threat to U.S. and international privacy rights and would put California out of step with privacy regulations throughout the U.S. and the world.

CONCLUSION

For the foregoing reasons, *Amici* ask this Court to deny Plaintiff's request for a preliminary injunction.

Dated: April 28, 2023

Respectfully submitted,

By: */s/ Alan Butler*

Alan Butler (SBN 281291)
butler@epic.org
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue NW
Washington, DC 20036
Tel: 202.483.1140

Meetali Jain (SBN 214237)
meetali@reset.tech
RESET TECH
1200 17th St NW, Suite 501
Washington, DC 20036

Attorneys for Proposed Amicus Curiae Electronic Privacy Information Center, Reset Tech, Frances Haugen, and Former Government Officials