No. 23-2969

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NETCHOICE, LLC, doing business as NetChoice,

Plaintiff - Appellee,

v.

ROB BONTA, 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

BRIEF OF THE LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Jon Greenbaum
David Brody
Marc Epstein
LAWYERS' COMMITTEE FOR
CIVIL RIGHTS UNDER LAW
1500 K St. NW, Suite 900
Washington, DC 20005
(202) 662-8600
jgreenbaum@lawyerscommittee.org

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Amicus is a nonprofit organization. It has no parent corporations, and no publicly held corporation owns any portion of it.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Regulations

INTERESTS OF THE AMICUS CURIAE

Formed in 1963, the Lawyers' Committee for Civil Rights Under Law is a nonpartisan, nonprofit organization using legal advocacy to pursue racial justice. It fights inside and outside the courts to ensure that Black people and other people of color have the voice, opportunity, and power to make the promises of American democracy real. The Lawyers' Committee's Digital Justice Initiative works at the intersection of racial justice, technology, data, and privacy. The Initiative combats online discrimination and unfair or deceptive data practices targeting Black Americans and other communities of color. It regularly participates in cases involving online privacy and civil rights. *See*, *e.g.*, *NetChoice, LLC v. Paxton*, No. 22-555, *Moody v. NetChoice, LLC*, No. 22-277 (U.S. 2023); *Gonzalez v. Google LLC*, 598 U.S. 617 (2023); *Vargas v. Facebook, Inc.*, No. 21-16499 (9th Cir. 2023); *Liapes v. Facebook, Inc.*, 95 Cal. App. 5th 910 (1st Dist. 2023); *Opiotennione v. Facebook, Inc.*, No. 19-cv-07185, 2020 WL 5877667 (N.D. Cal. Oct. 2, 2020); *Dumpson v. Ade*, No. 18-cv-01011, 2019 WL 3767171 (D.D.C. Aug. 9, 2019).[1]

[1] Lawyers' Committee files this brief with the consent of all parties. No counsel for a party authored this brief in whole or in part. No person or entity, other than *amicus curiæ*, its members, or its counsel, made any monetary contribution to the preparation or submission of this brief.

INTRODUCTION

The district court's opinion erroneously expanded the scope of First Amendment scrutiny to cover unprotected speech and conduct and then misapplied First Amendment scrutiny, thus striking down a law protecting Black people and other people of color from data-driven discrimination and protecting privacy rights. The standard it adopted would endanger the ability to regulate online businesses in general. Not all information-processing activities are speech and a business's use of the internet does not transform routine commercial conduct into protected speech. Online businesses, even those engaged in publishing, do not have any "special immunity" under the First Amendment from laws of general applicability. *Pittsburgh Press Co. v. Pittsburgh Comm'n on Hum. Rel.*, 413 U.S. 376, 382 (1973) (internal quotation omitted).

Centuries of systemic discrimination, including slavery, Jim Crow, redlining, and subjugation through discrimination and intimidation, manifest in societal data that algorithms often recklessly replicate. Black people and other people of color feel the effects of "data-driven discrimination" in lower mortgage approval and refinancing rates, higher insurance rates, and unequal access to healthcare. Because of algorithms that intentionally or unintentionally consider race, children of color are excluded from schools and flagged as "high risk" of dropping out or committing

crimes. Laws regulating the use of privacy-invasive data practices play a vital role in protecting civil rights.

States are increasingly seeking to address these and other online harms. California's Age-Appropriate Design Code Act (CAADCA) does so in several ways, including, *inter alia*, privacy protections, impact assessments, and prohibitions of deceptive practices called "dark patterns." First, CAADCA protects privacy with "data minimization" provisions requiring that covered businesses not "[c]ollect, 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," except in limited circumstances. Cal. Civ. Code § 1798.99.31(b)(3); *see also id.* § 1798.99.31 (b)(1), (4)–(6), (8). Second, CAADCA requires that a covered business conduct a Data Protection Impact Assessment ("DPIA"), in which the business must "identify the purpose of the online service, product, or feature [that is likely to be accessed by children], 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." *Id.* § 1798.99.31 (a)(1)(B). Third, CAADCA prohibits certain uses of dark patterns on children, *id.* § 1798.99.31 (b)(7), and requires that covered businesses configure default privacy settings provided to children to offer higher levels of privacy, *id.* § 1798.99.31(a)(5)–(6).

The district court erroneously struck down these provisions.[2] The district court should not have applied intermediate First Amendment scrutiny to CAADCA's data minimization provisions. And even if the district court was correct in applying intermediate scrutiny to CAADCA's remaining provisions, *see* Appellant's Br. 32–40, they should have survived.

The district court's first error lies in holding CAADCA's data minimization provisions merit intermediate First Amendment scrutiny merely because they "restrict[] the collection and sharing of information." 1-ER-11–12. Many laws implicate First Amendment activity in some way, particularly internet laws, but not all laws regulating conduct trigger First Amendment scrutiny. *See, e.g.*, *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 706 (1986) ("[E]very civil and criminal remedy imposes some conceivable burden on First Amendment protected activities."). The district court specifically erred in relying on *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011). In that case, the Supreme Court invalidated a Vermont law that, unlike CAADCA, contained restrictions intended to favor the Vermont legislature's own viewpoint at the expense of a specific industry group. *Id.* at 571. *Sorrell* does not vitiate privacy regulations generally; in fact, the Court says that other types of privacy regulations may be perfectly fine. *See id.* at 571, 573, 579. In contrast, the

[2] The district court also struck down other CAADCA provisions, such as its age verification requirements. *See* Cal. Civ. Code § 1798.99.31(a)(5). *Amicus* takes no position on CAADCA provisions other than those discussed in this brief.

district court's erroneous analysis endangers numerous other laws regulating data privacy and protecting Black people from discrimination and other harms, from newer state privacy laws to longstanding federal laws like the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1320d-6, Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. § 1681 *et seq.*, Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510 *et seq.*, Communications Act of 1934, 47 U.S.C. § 605 *et seq.*, and Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 *et seq*.

The district court also erred in its application of intermediate scrutiny to CAADCA, jeopardizing additional categories of consumer protection laws. The district court erroneously required California to show that CAADCA would have no incidental burden on speech. Further, the district court struck down CAADCA's DPIA requirement without considering the basic benefits of transparency requirements and impact assessments. Impact assessments, whether focused on privacy impacts or discriminatory impacts, are essential to addressing bias and discrimination. They make businesses think proactively about how their products and systems operate, leading to design interventions to prevent and mitigate harms.

CAADCA also contains several prophylactics against online unfair and deceptive practices. It is well established that such policies generally do not run afoul of the First Amendment. *See, e.g.*, *United States v. Alvarez*, 567 U.S. 709, 723 (2012)

(plurality); *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 501 (1996). Black people and other people of color are disproportionately harmed by predatory data practices. The district court erred in invalidating CAADCA despite its constitutionally permissible regulation of unfair and deceptive practices.

The district court's expansion of the scope of First Amendment protected activity risks eviscerating privacy laws, transparency laws, and other efforts to regulate online commerce. Its ruling would disproportionately harm Black people and other people of color by impeding the ability to combat data-driven discrimination.

ARGUMENT

I. Discriminatory Data Practices and Algorithms Reinforce Historical Segregation and Inequities.

Data protection and privacy laws are necessary to protect Black people and other people of color, particularly children of color, from data-driven discrimination. Black people and other people of color have experienced generations of institutionalized discrimination, including slavery, segregation, redlining, and disenfranchisement. The effects of discrimination continue to divide society "along [the same] lines of color," in "investment in construction; urban blight; real estate sales; household loans; small business lending; public school quality; access to transportation; access to banking; access to fresh food; life expectancy; asthma rates; lead paint exposure rates; diabetes rates; heart disease rates; and the list goes on."

Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 349 (4th Cir. 2021) (Gregory, C.J., concurring). When poorly designed algorithms ingest societal data reflecting racial biases, without adequate safeguards, they often reproduce and amplify discrimination. *See, e.g.*, *The New Invisible Hand? The Impact of Algorithms on Competition and Consumer Rights: Hearing Before the S. Comm. on the Judiciary*, 118th Cong. (Dec. 13, 2023) (written statement of Damon T. Hewitt, President & Exec. Dir., Lawyers' Committee for Civil Rights Under Law, at 15–50) (Appendix I, cataloguing over 100 examples of data-driven harms to equal opportunity).[3]

Online businesses collect personal data from an unequal starting point and replicate the discriminatory outcomes in their technologies. This is true in almost every facet of society, including housing, *see, e.g.*, Shawn Donnan et al., *Wells Fargo Rejected Half Its Black Applicants in Mortgage Refinancing Boom*, Bloomberg (Mar. 11, 2022) (Wells Fargo's mortgage refinancing algorithms rejected over half of Black applicants while approving over 70% of white applicants);[4] employment, *see, e.g.*, Muhammad Ali et al., *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes*, 3 Proc. ACM on Human-

[3] https://www.judiciary.senate.gov/imo/media/doc/2023-12-13_pm_-_testimony_-_hewitt.pdf.

[4] https://www.bloomberg.com/graphics/2022-wells-fargo-black-home-loan-refinancing.

Computer Interaction, No. 199 (Nov. 2019) (Meta delivered ads for positions in the lumber industry to over 90% men and over 70% white users and ads for janitors to over 65% women and over 75% Black users);[5] credit and finance, *see, e.g.*, Robert Bartlett et al., *Consumer-Lending Discrimination in the FinTech Era* (Nat'l Bureau Econ. Rsch. Working Paper No. 25943, 2019) (FinTech algorithms charge otherwise equivalent Black and Latino borrowers higher rates);[6] insurance, *see, e.g.*, Julia Angwin et al., *Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk*, ProPublica (Apr. 5, 2017) (Black and Brown neighborhoods systematically charged higher car insurance premiums than white neighborhoods of similar risk);[7] and healthcare, *see, e.g.*, Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 Sci. 447 (2019) (algorithm underpredicted sickness in Black patients compared to white patients).[8]

The district court wrongly suggested—supplanting its policy judgment over the legislature's—that minors from "vulnerable populations" are somehow exempt from these harmful effects. 1-ER-30 (noting that "profiling and subsequent targeted content can be beneficial to minors, particularly those in vulnerable populations").

---

[5] https://dl.acm.org/doi/10.1145/3359301.
[6] https://www.nber.org/papers/w25943.
[7] https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk.
[8] https://www.science.org/doi/10.1126/science.aax2342.

Even just with respect to education, the effects of data-driven discrimination are profound. Some schools have used personal data deliberately to advertise to white students. Todd Feathers, *College Prep Software Naviance Is Selling Advertising Access to Millions of Students*, The Markup (Jan. 13, 2022).[9] Algorithms used to determine admission "regularly screened out" Black and Latino students from New York City's top performing high schools. Colin Lecher & Maddy Varner, *NYC's School Algorithms Cement Segregation. This Data Shows How*, The Markup (May 26, 2021).[10] Algorithms used in Wisconsin to determine whether students were "high risk" for not graduating on time generated more false alarms about Black and Latino students than white students. Todd Feathers, *False Alarm: How Wisconsin Uses Race and Income to Label Students "High Risk"*, The Markup (Apr. 27, 2023);[11] *see also* Todd Feathers, *Major Universities Are Using Race as a "High Impact Predictor" of Student Success*, The Markup (Mar. 2, 2021).[12]

There are numerous examples in other domains. Child welfare agencies used algorithms that had "a pattern of flagging a disproportionate number of Black

[9] https://themarkup.org/machine-learning/2022/01/13/college-prep-software-naviance-is-selling-advertising-access-to-millions-of-students.
[10] https://themarkup.org/machine-learning/2021/05/26/nycs-school-algorithms-cement-segregation-this-data-shows-how.
[11] https://themarkup.org/machine-learning/2023/04/27/false-alarm-how-wisconsin-uses-race-and-income-to-label-students-high-risk.
[12] https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success.

children for a 'mandatory' neglect investigation, when compared with white children." Sally Ho & Garance Burke, *An Algorithm That Screens for Child Neglect Raises Concerns*, AP News (Apr. 29, 2022).[13] Police in Florida used a data-driven program to identify people it suspects may commit future crimes, using data that were likely biased and causing officers to target and arrest minors. Kathleen McGrory & Neil Bedi, *Targeted*, Tampa Bay Times (Sept. 3, 2020).[14] A common healthcare algorithm used to determine whether pediatric patients needed to be taken to emergency departments was more likely to flag Black and Latino children's emergency department visits as "low-acuity or non-emergent as compared to visits [by] white children," potentially leading to lower insurance payments for those visits. Frank Diamond, *Algorithm Used to Cut ER Overutilization for Kids Penalizes Black, Hispanic Patients: Study*, Fierce Healthcare (May 10, 2023).[15]

Data-driven discrimination harms Black people and other people of color, particularly children of color, and laws regulating algorithmic bias and online business practices are necessary to protect against it.

---

[13] https://apnews.com/article/child-welfare-algorithm-investigation-9497ee937e0053ad4144a86c68241ef1.
[14] https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/.
[15] https://www.fiercehealthcare.com/payers/method-used-cut-emergency-department-overutilization-kids-penalizes-blacks-hispanics-study.

II. The District Court's Erroneous First Amendment Analysis Imperils Laws That Protect Black People From Data-Driven Discrimination and Other Harms.

The Court erred in its application of the First Amendment to CAADCA in several ways, upending decades of precedent and jeopardizing numerous laws in the process. *First*, the district court erred in holding that CAADCA's data minimization provisions, *see* Cal. Civ. Code § 1798.99.31(b)(1), (3)–(6), (8), merit First Amendment intermediate scrutiny. Like many privacy laws governing data use before it, CAADCA regulates non-expressive conduct and falls outside the First Amendment. If the Court upholds the district court's erroneous interpretation of the First Amendment, numerous laws regulating the collection, use, and sharing of information may fall under unwarranted scrutiny, threatening privacy protections at both the state and federal levels that Americans have taken for granted for decades. *Second*, the district court erred in its application of intermediate scrutiny, endangering commercial regulations that have any incidental burden on speech. *Third*, when applying intermediate scrutiny, the district court ignored the accountability benefits of transparency laws and impact assessment requirements. *Fourth*, the district court did not follow controlling precedent upholding unfair and deceptive practices laws and failed to recognize CAADCA's benefits in preventing such harms when they occur online.

A. The district court erred in holding that CAADCA's privacy provisions merited and failed First Amendment scrutiny.

CAADCA helps mitigate the inequities described in Section I by restricting the ability of online businesses to collect, sell, share, or retain children's data. *See* Cal. Civ. Code § 1798.99.31(b)(1), (3)–(6), (8). The district court incorrectly held that intermediate First Amendment scrutiny applies to these data minimization provisions. *See* 1-ER-12–13. Its misapplication of First Amendment scrutiny threatens numerous laws that have stood on years of precedent.

1. Data minimization laws regulate non-expressive conduct.

The district court incorrectly held that First Amendment intermediate scrutiny applies to CAADCA's data minimization provisions because they "restrict[] the collection and sharing of information." 1-ER-12. First Amendment protection extends "only to conduct that is inherently expressive." *Rumsfeld v. F. for Acad. & Institutional Rts., Inc.*, 547 U.S. 47, 66–67 (2006). Indeed, many laws restrict the collection and sharing of information in some way. *See, e.g.*, *Univ. of Pennsylvania v. Equal Emp. Opportunity Comm'n*, 493 U.S. 182, 200 (1990) ("[M]any laws make the exercise of First Amendment rights more difficult."); *Arcara*, 478 U.S. at 706 ("[E]very civil and criminal remedy imposes some conceivable burden on First Amendment protected activities."). Thus, the Supreme Court has rejected the notion "that an apparently limitless variety of conduct can be labeled 'speech' whenever the

person engaging in the conduct intends thereby to express an idea." *United States v. O'Brien*, 391 U.S. 367, 376 (1968).

Just because a business operates online, even if it is involved in publishing, does not give it "special immunity" from laws of general applicability. *Pittsburgh Press Co.*, 413 U.S. at 382 (cleaned up). "As [online media] has evolved from an assortment of small [websites] into a diverse aggregation including large publishing empires as well, the parallel growth and complexity of the [online] economy have led to extensive regulatory legislation from which the publisher of a [website] has no special immunity" under the First Amendment. *Id.* (cleaned up).

For these reasons, countless laws regulating non-expressive conduct in all manner of sectors have bypassed or survived First Amendment scrutiny. For example, antitrust laws, anti-solicitation laws, the Fair Labor Standards Act, the National Labor Relations Act, and other laws do not run afoul of the First Amendment even as applied to the press. *See Minneapolis Star & Trib. Co. v. Minn. Comm'r of Revenue*, 460 U.S. 575, 581 (1983) (collecting cases). Public health laws may force the closure of a bookstore. *Arcara*, 478 U.S. at 698. A ban on race-based hiring "may require employers to remove 'White Applicants Only' signs"; "'an ordinance against outdoor fires' might forbid 'burning a flag'"; and "antitrust laws can prohibit 'agreements in restraint of trade.'" *Sorrell*, 564 U.S. at 567 (citations omitted). The list goes on. *See, e.g.*, *Nat'l Endowment for the Arts v. Finley*, 524 U.S.

569, 580–81 (1998) (grant making procedural requirements); *Leathers v. Medlock*, 499 U.S. 439, 447 (1991) (sales tax on cable television services); *Univ. of Pennsylvania*, 493 U.S. at 201 (disclosure of peer-reviewed materials).

Data minimization laws are a type of privacy law that regulate non-expressive conduct. They regulate the type of information companies can collect, how long they can hold onto that information, with whom the businesses can share that information, and for what purposes. Data minimization laws recognize that the unnecessary or disproportionate accumulation of data itself often leads to societal harms, and these laws apply generally to all kinds of businesses. *See supra* Section I; *Sorrell*, 564 U.S. at 579; *Whalen v. Roe*, 429 U.S. 589, 605 (1977) ("We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks.").

The district court largely relied on *Sorrell* in coming to the opposite conclusion, but its reading of *Sorrell* is overbroad and its application to this case flawed. *Sorrell* involved a Vermont law that restricted the ability of pharmacies, health insurers, and similar entities to sell, disclose, or use pharmacy records containing information about physicians' prescription practices. *Sorrell*, 564 U.S. at 558–59. The Court held that the Vermont law merited and failed intermediate scrutiny because it imposed a "specific, content-based burden on protected expression" on one group of people: pharmaceutical manufacturers. *Id.* at 564–65.

The Court reasoned that Vermont was attempting to "hamstring the opposition" by blocking the drug promoters from accessing and using the prescriber-identifying information "even while the State itself can use the information" to advance its own countervailing message. *Id.* at 578, 580. Although the Court noted that there also was "a strong argument that prescriber-identifying information is speech for First Amendment purposes," it held there was "no need" to decide the issue because the law's content- and speaker-based restrictions were decisive. *Id.* at 570–71.

The district court's application of *Sorrell* is flawed in at least three ways. First, the Vermont law, unlike CAADCA, did not govern the collection or retention of information. *Id*. at 558–59. It merely prevented pharmacists from passing on information that they had collected. *See id.* Thus, *Sorrell* provides no guidance for CAADCA's restrictions on the collection and retention of data.

Second, the Vermont law was unjustified viewpoint discrimination based on the identity of the actor. *See id.* at 571. It "burden[ed] the speech" of a select and disfavored group of people (pharmaceutical manufacturers) even while allowing others—including the state—to engage in the same conduct uninhibited, all "to tilt public debate" in the state's "preferred direction." *Id*. at 578–79. CAADCA, however, does not target conduct by one group of people or businesses to favor the state on a niche policy issue. CAADCA applies broadly to any "business that provides an online service, product, or feature likely to be accessed by children."

Cal. Civ. Code § 1798.99.31(b); *cf. Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 661 (1994) (upholding regulations that were "broad based, applying to almost all cable systems in the country, rather than just a select few"); *Leathers*, 499 U.S. at 449 (holding tax that "affected approximately 100 suppliers of cable television services" was "not a tax structure that resembles a penalty for particular speakers or particular ideas").

Third, the Supreme Court held that the Vermont law was not really about protecting data at all—and acknowledged that a truly privacy-protective law could have survived. *See Sorrell*, 564 U.S. at 573. It assumed that the prescriber-identifying information at issue was "a mere commodity" and noted that "[t]he capacity of technology to find and publish personal information" presented "serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure." *Id.* at 571, 579. The Court even indicated that the types of regulations it was invalidating may have survived if the state had passed "a more coherent policy," such as one allowing disclosure of the information "in only a few narrow and well-justified circumstances" like in HIPAA. *Id.* at 573. "A statute of that type would present quite a different case from the one presented here." *Id*. CAADCA's data minimization provisions are that "more coherent policy." *Id.*

2. The reasoning of the district court's decision would endanger federal and state privacy laws.

The district court's incorrect interpretation of the First Amendment and misapplication of *Sorrell* endangers myriad federal and state privacy laws. And by endangering privacy laws, the district court imperils the civil rights of Black people and other people of color. Privacy rights are civil rights; they prevent one's personal information from being used against oneself unfairly. *See, e.g.*, *U.S. Dep't of Just. v. Reps. Comm. for Freedom of Press*, 489 U.S. 749, 766 (1989) (relying on the "strong privacy interest" in the "nondisclosure of compiled computerized information"); *Whalen*, 429 U.S. at 607 (Brennan, J., concurring) ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information."). The "inviolability of privacy" is "indispensable to preservation of freedom of association." *NAACP v. State of Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958).

Federal privacy laws have regulated the collection and disclosure of information for almost 100 years, but the district court's decision calls them into question. There is a direct connection between many of these laws and the prevention of harm against Black people and other people of color.

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) prohibits the disclosure of individually identifiable health information without patient consent. *See* 42 U.S.C. § 1320d-6. It protects the privacy of Black women, who face significantly higher rates of criminalization when seeking reproductive health care, leading

many to forego seeking the care they need. Hum. Rts. Watch et al., *Human Rights Crisis: Abortion in the United State After Dobbs* (Apr. 18, 2023);[16] Lynn M. Paltrow, *Arrests of and Forced Interventions on Pregnant Women in the United States*, *1973–2005: Implications for Women's Legal Status and Public Health*, 38 J. Health Pol., Pol'y, & L. 299, 311 (2013).

- The Fair Credit Reporting Act of 1970 (FCRA) limits the information credit bureaus can collect, how they collect it, to whom they provide the information, and for what purposes. *See* 15 U.S.C. § 1681 *et seq*. As the Federal Trade Commission (FTC) has found, identity theft disproportionately impacts communities of color and low-income consumers are less likely to have the resources to bounce back after experiencing fraud. *See* FTC, *Serving Communities of Color: A Staff Report on the Federal Trade Commission's Efforts to Address Fraud and Consumer Issues Affecting Communities of Color* (2021) [hereinafter FTC, *Serving Communities of Color*];[17] *see also* Sarah Dranoff, *Identity Theft: A Low-Income Issue*, Am. Bar Ass'n (Dec. 15, 2014).[18]

- The Family Educational Rights and Privacy Act of 1974 (FERPA) prohibits educational institutions from disclosing personally identifiable information in education records without student or parent consent. 20 U.S.C. § 1232g(b). Online and for-profit colleges have specifically targeted Black and Latino prospective students with predatory marketing practices while providing low-quality education and leaving people with high debt. Genevieve (Genzie) Bonadies et al., *For-Profit Schools' Predatory Practices and Students of Color: A Mission to Enroll Rather than Educate*, Harv. L. Rev. Blog (July 30, 2018).[19]

---

[16] https://www.hrw.org/news/2023/04/18/human-rights-crisis-abortion-united-states-after-dobbs.

[17] https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf.

[18] https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue/.

[19] https://blog.harvardlawreview.org/for-profit-schools-predatory-practices-and-students-of-color-a-mission-to-enroll-rather-than-educate/.

- The Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 *et seq.*, limits the ability of online providers to collect personal information from children. *See* 15 U.S.C. § 6502. In minimizing data collection and retention, COPPA inhibits data-driven discrimination in similar ways to CAADCA. *See supra* Section I.

These are not the only federal privacy laws that the opinion below would call into question. Going at least as far back as the Communications Act of 1934 and continuing through the Electronic Communications Privacy Act of 1986, Congress has restricted nonconsensual recording or disclosure of electronic communications. *See* 47 U.S.C. § 605; 18 U.S.C. § 2511. Even the wrongful disclosure of video rental or sale records is prohibited under the Video Privacy Protection Act of 1988. 18 U.S.C. § 2710.

The district court's reasoning also would upend state laws regulating data privacy. For example, the California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100, requires:

> A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

Several states, including Colorado, Connecticut, and Virginia, have passed laws with data minimization requirements. *See, e.g.*, Colo. Rev. Stat. § 6-1-1308(3); Conn. Gen. Stat. § 42-520(a); Va. Code Ann. § 59.1-578(A). Indeed, at least 13 states

recently have enacted comprehensive privacy laws. *See* LewisRice, *U.S. State Privacy Laws*.[20] Likewise, some states, like Illinois, Texas, and Washington, have passed laws regulating the retention, collection, disclosure, and destruction of biometric identifiers like a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. *See, e.g.*, 740 Ill. Comp. Stat. 14/1 *et seq.*; Tex. Bus. & Com. Code § 503.001; Wash. Rev. Code § 19.375.010 *et seq.* Research has established that many of these technologies, such as facial recognition algorithms, are racially-biased, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learning Rsch. 1, 12 (2018),[21] and their use has caused the wrongful arrests of innocent Black people. *See, e.g.*, Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. Times (Aug. 6, 2023);[22] John Simerman, *JPSO Used Facial Recognition Technology to Arrest a Man. The Tech Was Wrong.*, The Times-Picayune/New Orleans Advoc. (Jan. 2, 2023);[23] Khari Johnson, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, WIRED (Feb. 28, 2023).[24]

---

[20] https://www.lewisrice.com/u-s-state-privacy-laws/ (last visited Dec. 20, 2023).
[21] https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[22] https://www.nytimes.com/2023/08/06/technology/facial-recognition-false-arrest.html.
[23] https://www.nola.com/news/crime_police/jpso-used-facial-recognition-to-arrest-a-man-it-was-wrong/article_0818361a-8886-11ed-8119-93b98ecccc8d.html.
[24] https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/.

The district court erroneously held that CAADCA's privacy provisions require First Amendment scrutiny, sweeping in numerous federal and state privacy laws and endangering the civil rights of Black people and other people of color in the process.

B. The district court failed to recognize that commercial laws of general applicability may impose incidental burdens on speech.

Even if provisions of CAADCA implicate protected speech, the district court misapplied the standard of review, producing absurd results.

The district court noted throughout its decision that it was concerned with the detrimental effect CAADCA would have on protected speech. 1-ER-24, 26, 29–31. It struck down CAADCA's high-default privacy settings requirement because it would cause some businesses to prohibit children from accessing their services altogether, 1-ER-26; its prohibitions on profiling children by default and the unauthorized use of children's personal information because (contrary to overwhelming research, *see supra* Section I), the court decided that some targeted advertising is beneficial to minors, *see* 1-ER-30, 32; its prohibitions on the use of dark patterns because "some content that might be considered harmful to one child may be neutral at worst to another," *see* 1-ER-35; and its data minimization provisions because they "would restrict neutral or beneficial content," 1-ER-31–32.

In making these conclusions, the district court failed to recognize that "incidental burdens on speech" are permissible when a regulation is directed at commerce, as is the case here. *Sorrell*, 564 U.S. at 567. The end result of the district

court's reasoning is that a privacy law can only be constitutional if it laser-cuts around any possible neutral or beneficial activity—even wholly speculative scenarios—and only regulates conduct universally recognized as harmful. That is not what intermediate scrutiny requires. Intermediate scrutiny requires "a fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition but one whose scope is in proportion to the interest served." *Greater New Orleans Broad. Ass'n, Inc. v. United States*, 527 U.S. 173, 188 (1999). Thus, the proponent of a challenged regulation need only demonstrate that it "carefully calculated the costs and benefits associated with the burden on speech imposed by its prohibition." *Id.* (internal quotation omitted). These safeguards are important so that the district court does not conduct its own abbreviated policy determinations and substitute them for the reasoned policy determinations of the legislature—as it did here.

The district court's rule would cripple legislators and lead to absurd results. For example, the federal Do-Not-Call Registry is not unconstitutional just because *some* non-exempt solicitors may offer benevolent services. *See* 15 U.S.C. § 6151 *et seq.* Ballot secrecy laws are not invalid merely because *some* businesses may want to identify partisans to whom to market political merchandise. *Cf. Burson v. Freeman*, 504 U.S. 191, 206 (1992) (plurality) (noting that "all 50 States, together with numerous other Western democracies" use "a secret ballot" to protect against

voter intimidation and election fraud). Laws prohibiting private sector wiretapping, *see, e.g.*, 47 U.S.C. § 605 (prohibiting telecommunications providers from recording phone calls without consent), surely impair some beneficial data uses. Instances in which data regulations have no other consequences are few and far between, but that does not nullify "the right to be let alone" in those circumstances. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 1890 Harv. L. Rev. 193 (1890).[25] The district court misunderstood and misapplied controlling First Amendment precedent on how to evaluate a commercial regulation.

C. The district court improperly applied intermediate scrutiny by failing to recognize the benefits of transparency and impact assessment laws.

The district court's misapplication of First Amendment doctrine to CAADCA's transparency and impact assessment provisions jeopardizes numerous consumer protection regimes that prevent discrimination and foster accountability.

The district court invalidated CAADCA's DPIA requirement in part because CAADCA's DPIA requirement does not require businesses to adhere to any plan to mitigate the risks identified in their report. *See* 1-ER-22. This reasoning is absurd. As Justice Brandeis commented over 100 years ago, "Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of

[25] https://www.jstor.org/stable/1321160.

disinfectants; electric light the most efficient policeman." Louis D. Brandeis, *What Publicity Can Do*, Harper's Weekly, at 10 (Dec. 20, 1913).

The district court's decision ignores the basic benefits of impact assessments and transparency requirements. These requirements are not intended to *force* companies to rectify their underlying risks in a direct and prescriptive manner. Rather, assessments and disclosures compel companies to consider the impact of their actions and align corporate incentives with the public welfare. In other words, when companies have to examine harms they may cause and disclose what they find, they are likely to want to fix those harms voluntarily and proactively—or risk opprobrium and other negative consequences. Further, transparency requirements like CAADCA's DPIA requirement, which requires that companies make available their DPIA reports to the state upon written request, Cal. Civ. Code § 1798.99.31(a)(4)(A), empower the government to hold deficient companies accountable through enforcement actions and assess whether additional regulation is needed. In this way, like data minimization laws, impact assessment and transparency requirements inhibit data-driven discrimination and other discriminatory harms impacting Black people and other people of color. *See supra* Section I.

The reasoning of the district court's decision would threaten many other laws that require impact assessments and disclosures. For example, some localities

require employers to conduct bias audits within one year of using an automated employment tool. *See, e.g.*, N.Y.C. Admin. Code § 20-871(a)(1). The Securities and Exchange Commission promulgates rules requiring companies to disclose "risk factors" to the public to protect investors—but the companies do not need to eliminate those risks. *See* 17 C.F.R. § 229.105. Some state laws require the filing of a health equity impact assessment when seeking to establish a health care facility, but the impact assessment does not require entities to solve the adverse impacts identified in their assessments. *See, e.g.*, N.Y. Pub. Health Law § 2802-b. The Nutrition Labeling and Education Act of 1990 requires companies to provide food labels—the ubiquitous "Nutrition Facts" boxes on every grocery store item—but it doesn't require companies to make unhealthy foods healthy. 21 U.S.C. § 343(q). And several other states have passed privacy laws with DPIA requirements, none of which requires the reporting entity to adhere to the solution proposed in their DPIA report. *See, e.g.*, Colo. Rev. Stat. § 6-1-1309; Conn. Gen. Stat. § 42-522; Va. Code Ann. § 59.1-580. The White House has also recently hailed the importance of impact assessments for preventing discrimination by automated decision-making systems in its *Blueprint for an AI Bill of Rights*, White House Off. of Sci. & Tech. Pol'y, *Blueprint for an AI Bill of Rights* (2022),[26] the Office of Management and Budget

[26] https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

has proposed requiring agencies to conduct AI impact assessments, Off. of Mgmt. & Budget, Exec. Off. of the President, Proposed Memorandum, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* at 15–16, 18–19 (proposed Nov. 1, 2023),[27] and the National Institute of Standards and Technology has developed a Risk Management Framework for advancing trustworthy and responsible AI use and development, Nat'l Inst. of Standards & Tech., U.S. Dep't of Com., NIST AI 100-1, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Jan. 2023).[28]

The district court's decision ignores the basic premise of transparency—that sunlight is the best disinfectant. Its decision is detached from First Amendment precedent and endangers impact assessment and transparency requirements in numerous other laws.

D. The district court erroneously struck down CAADCA's regulation of unfair and deceptive practices.

The district court erroneously disregarded the constitutionality of laws regulating unfair and deceptive practices when it invalidated CAADCA's regulation of dark patterns, data minimization provisions, and disclosure requirements,

[27] https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf.
[28] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

imperiling hundred-year-old legal principles that were used to dismantle Jim Crow segregation.

It is well-established that the First Amendment permits regulation of unfair and deceptive practices. The "governmental power ["to protect people against fraud"] has always been recognized in this country and is firmly established." *Donaldson v. Read Mag.*, 333 U.S. 178, 190 (1948); *see also, e.g.*, *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 563 (1980) ("The government may ban forms of communication more likely to deceive the public than to inform it. . . ."). Thus, "[w]hen a State regulates commercial messages to protect consumers from misleading, deceptive, or aggressive sales practices, or requires the disclosure of beneficial consumer information, the purpose of its regulation is consistent with the reasons for according constitutional protection to commercial speech and therefore justifies less than strict review." *44 Liquormart, Inc*, 517 U.S. at 501; *see also, e.g.*, *Alvarez*, 567 U.S. at 717 (plurality) (holding fraud is not entitled to First Amendment protection). Congress has promulgated numerous laws on this basis. *See, e.g.*, 15 U.S.C. § 45 (FTC Act); 47 U.S.C. § 202(a) (Communications Act of 1934); 12 U.S.C. § 5531 (Dodd-Frank Act).

The district court rejected the premise that dark patterns constitute "real harm." 1-ER-27; *see also, e.g.*, 1-ER-33 (holding California "has not shown a harm resulting from the provision of more personal information 'beyond what is

reasonably expected' for the covered business to provide its online service, product, or feature"); 1-ER-34 (noting examples of dark patterns were "not causally connected to an identified harm"). But there is no question dark patterns are a harmful unfair and deceptive practice. Dark patterns are the deliberate misleading of users by "obscuring, subverting, or impairing consumer autonomy, decision-making, or choice" to deceive consumers into giving away their personal data. FTC, *Bringing Dark Patterns to Light: An FTC Workshop* (Apr. 29, 2021).[29] Examples of dark patterns include online subscriptions and free trials that make it difficult for a user to unsubscribe, deceptively labeled buttons to induce consumer consents, and graphical elements that direct users' attention away from certain options on a website. Jasmine McNealy, *What Are Dark Patterns? An Online Media Expert Explains*, Nextgov/FCW (Aug. 3, 2021).[30]

As California argues, dark patterns "subvert[] or impair[] user autonomy, decision-making, or choice," Appellant's Br. at 15; they "manipulate or nudge the user . . . at the expense of the user's interests," 4-ER-696; and they "can make it difficult or impossible for children to avoid harmful content," 1-ER-33, or lead to "extreme content generation," Appellant's Br. at 7. Indeed, dark patterns are

[29] https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop.
[30] https://www.nextgov.com/ideas/2021/08/what-are-dark-patterns-online-media-expert-explains/184244/.

particularly predatory toward low-income users, people for whom English is a second language, people from nondominant cultures, and people with less digital literacy. *See* FTC, *Serving Communities of Color*, *supra*; Catherine Zhu, *Dark Patterns — A New Frontier in Privacy Regulation*, Reuters (July 29, 2021).[31]

The district court also struck CAADCA's data minimization and disclosure provisions even though they too prevent unfair and deceptive practices. *See* 1-ER-20–21 ("CAADCA regulates speech that is neither misleading nor related to unlawful activity."). Data-fueled unfair and deceptive practices are endemic and often harm Black people and other people of color. *See supra* Section I.

The district court's decision jeopardizes the ability to combat discrimination using unfair and deceptive practice authorities. Unfair and deceptive practices statutes have a long history in the struggle for civil rights. Such a provision in the Interstate Commerce Act was used to desegregate bus terminals and railroads, including the landmark 1960 decision in *Boynton v. Virginia* that catalyzed the Freedom Rides. *See Boynton v. Virginia*, 364 U.S. 454 (1960) (bus terminal segregation); *Henderson v. United States*, 339 U.S. 816 (1950) (dining car segregation); *Mitchell v. United States*, 313 U.S. 80 (1941) (railcar segregation); *Keys v. Carolina Coach Co.*, 64 M.C.C. 769 (Interstate Commerce Commission

[31] https://www.reuters.com/legal/legalindustry/dark-patterns-new-frontier-privacy-regulation-2021-07-29/.

1955) (bus segregation). The Federal Trade Commission also has invoked its unfair and deceptive practices authority in enforcement actions against race discrimination. *See, e.g.*, Public Statement, FTC, *Joint Statement of Chair Lina M. Khan, Commissioner Rebecca Kelly Slaughter, and Commissioner Alvaro M. Bedoya In the Matter of Passport Auto Group*, at 3 (Oct. 18, 2022) (auto sales);[32] *E.G. Reinsch, Inc.*, 75 F.T.C. 210 (1969) (housing advertisements); *First Buckingham Cmty., Inc.*, 73 F.T.C. 938 (1968) (housing advertisements). A similar provision in the Communications Act prohibits race and income discrimination in telecommunications. *See Orloff v. FCC*, 352 F.3d 415, 420 (D.C. Cir. 2003).

In rejecting the premise that states may regulate online unfair and deceptive practices, the district court casts doubt on laws that can combat discrimination and other harmful practices by the next generation of corporate actors.

CONCLUSION

The district court erred in its interpretation and application of First Amendment scrutiny to CAADCA, ignoring Supreme Court precedent and threatening decades-old laws that protect Black people and other people of color from data-driven discrimination and privacy violations. The Lawyers' Committee respectfully urges this Court to reverse the judgment of the district court.

[32] https://www.ftc.gov/system/files/ftc_gov/pdf/joint-statement-of-chair-lina-m.-khan-commissioner-rebecca-kelly-slaughter-and-commissioner-alvaro-m.-bedoya-in-the-matter-of-passport-auto-group.pdf.

Dated: December 20, 2023

Respectfully submitted,

By: s/ Jon Greenbaum

Jon Greenbaum
David Brody
Marc Epstein
LAWYERS' COMMITTEE FOR
CIVIL RIGHTS UNDER LAW
1500 K St. NW, Suite 900
Washington, DC 20005
(202) 662-8600
jgreenbaum@lawyerscommittee.org

Counsel for Amicus Curiae

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

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

I am the attorney or self-represented party.

This brief contains 6514 **words,** including 0 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.

[X] 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/ Jon Greenbaum **Date** 12/20/2023

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

CERTIFICATE OF SERVICE

I certify that on December 20, 2023, this brief was filed using the Court's CM/ECF system. All participants in the case are registered CM/ECF users and will be served electronically via that system.

s/ Jon Greenbaum
Jon Greenbaum