No. 23-2969

In the United States Court of Appeals
for the Ninth Circuit

ROB BONTA,
Defendant-Appellant,

v.

NETCHOICE, LLC,
Plaintiff-Appellee.

On Appeal from the United States District Court for the
Northern District of California, No. 5:22-cv-8861

BRIEF OF AMICUS CURIAE TECHFREEDOM IN SUPPORT OF PLAINTIFF-APPELLEE AND AFFIRMANCE

Corbin K. Barthold
TECHFREEDOM
1500 K Street NW
Washington, DC 20005
(771) 200-4997
cbarthold@techfreedom.org
Attorney for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

TechFreedom has no parent corporation, it issues no stock, and no publicly held corporation owns a ten-percent or greater interest in it.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

TABLE OF AUTHORITIES
(Cont.)

Page(s)

TABLE OF AUTHORITIES
(Cont.)

Page(s)

TABLE OF AUTHORITIES
(Cont.)

Page(s)

TABLE OF AUTHORITIES
(Cont.)

Page(s)

INTEREST OF AMICUS CURIAE*

TechFreedom is a nonprofit, nonpartisan think tank based in Washington, D.C. It is dedicated to promoting technological progress that improves the human condition. It seeks to advance public policy that makes experimentation, entrepreneurship, and investment possible.

TechFreedom opposes government efforts to control online speech. That is precisely why TechFreedom opposes laws that mandate online age verification or (what is functionally the same thing) age estimation. As TechFreedom's experts have explained in extensive expert commentary on, and analysis of, such laws, age verification/estimation erodes online anonymity and, in consequence, chills free speech and free association. See, e.g., Mike Masnick, *You Can't Wish Away the First Amendment to Mandate Age Verification*, Techdirt (Sept. 13, 2023), http://tinyurl.com/mtfhd9dp (discussing the work of TechFreedom attorney Ari Cohn); Corbin K. Barthold, *Republicans Can't Decide If They Want Online Privacy or Not*, The Daily Beast (Sept. 5, 2023), http://tinyurl.com/2s3hr42n; Corbin K. Barthold, *Closing the Digital*

---

* No party's counsel authored any part of this brief. No one, apart from TechFreedom and its counsel, contributed money intended to fund the brief's preparation or submission. All parties have consented to the brief's being filed.

Frontier, City Journal (Mar. 7, 2023), http://tinyurl.com/d5aree9m (discussing AB 2273).

INTRODUCTION & SUMMARY OF ARGUMENT

As the district court observed, AB 2273 requires a covered website either to estimate the age of users and provide "a high default privacy setting" to minors, or, absent such age estimation, to "provide the high default privacy setting to all users." 1-ER-15-16. A website that estimates users' ages (route one) must collect users' sensitive information. *Id.* at 24. A website that instead applies "high default privacy settings"—privacy controls fit for children—to everyone (route two) will avoid offering certain speech to adults that it would otherwise provide. *Id.* at 25. Down route one, the statute undermines its own putative end (privacy); down route two, the statute unduly chills speech. The upshot is that AB 2273's age estimation provision is not narrowly tailored. The district court ruled, therefore, that the provision violates the First Amendment.

That's the right result. But the district court could have gone further. Although the court was correct that a high privacy default (route two) would have "a vast chilling effect," 1-ER-24-25, *so would age estimation* (route one). A high privacy default chills *the covered website*—which offers less speech than it otherwise would. Age estimation chills

users—who visit fewer websites, speak at fewer websites, and speak less at websites than they otherwise would.

The district court understood that AB 2273 will chill users. 1-ER-16. In a section of its opinion shooting down California's argument that AB 2273 does not regulate speech at all, the court noted that age estimation creates friction ("time delays and other barriers to entry") that will frustrate users, causing them to leave websites without accessing and viewing any content. *Id*. But such friction is only a small part of the overall chilling effect that age estimation will have on users.

A wide range of experts, politicians, and public intellectuals are informing the public of the risks that come with sharing information online. These observers view the matter through different ideological lenses, and they underscore different dangers. But their distinct voices combine into a unified message: Users should beware of letting a website gratuitously collect personal information. It is reasonable to assume that this message, coming at the public from many sources and many directions, is sinking in with a non-negligible portion of Internet users.

More than ever, therefore, any information-collection measure that imperils users' privacy and anonymity—as age estimation does—is likely to have "a vast chilling effect," 1-ER-24, on online speech.

This brief reviews the diverse warnings the public has been receiving about the perils of undue data collection. Although the warnings do not always fit into neat categories, this brief will, for the sake of conceptual clarity, divide commentators into a "left" group and a "right" group. The ideological left fears that digital surveillance will promote corporate power and destroy personal privacy. The ideological right fears that digital surveillance will promote the monitoring of "social credit" and enable political oppression. Although their fears are distinct, the two sides arrive at the same place: a belief that users should jealously guard their online anonymity. Both sides warn that anonymity can be lost through the mishandling or misuse of supposedly protected data.

To alter public behavior, these concerns need not be accurate in every particular. (To make its point, this brief need not claim that a social credit system is in fact around the corner.) What matters is that the public has growing and rational (if not watertight) worries about giving up online anonymity, and that, given these worries, age estimation would, if implemented, have a "real and pervasive" deterrent effect on online speech and association. *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2388 (2021). "The *risk* of a chilling effect on association is enough, because First Amendment freedoms need breathing space to survive." *Id.* at 2389 (emphasis added) (cleaned up). As shown by the

extensive commentary, from both the left and the right, reviewed in this brief, AB 2273's age estimation rule creates just such a risk.

ARGUMENT

I. AB 2273's Age Estimation Provision Will Chill Leftwing Speech.

The left has a broad array of concerns about data collection and data privacy. It is claimed, on this side of the ideological spectrum, that "surveillance is everywhere in modern life." Julia Sonenshein, *How Surveillance Is Changing Our Most Intimate Relationships*, The New Republic (Jan. 28, 2024), http://tinyurl.com/3wtrvmt8. "Big Tech giants," in particular, purportedly "exploit people's data" and "invade Americans' privacy." Sara Morrison, *Elizabeth Warren Created a Federal Agency Once. Can She Do It Again?*, Vox (Sept. 14, 2023) (quoting Sen. Elizabeth Warren), http://tinyurl.com/43x4nawp. Some have gone so far as to contend that "data privacy" is "the next great civil rights struggle." William Davidow & Michael S. Malone, *Corporations Shouldn't Be Allowed to Own Your Personal Data at All*, Salon (Feb. 15, 2020), http://tinyurl.com/5n77ss3u.

Perhaps the most prominent voice on the privacy-concerned left is Shoshana Zuboff, the professor and author who mainstreamed the term

"surveillance capitalism." According to Zuboff, the last decade has "seen" the "wholesale destruction of privacy." Lauren Jackson, *Shoshana Zuboff Explains Why You Should Care About Privacy*, NY Times, (May 21, 2021), http://tinyurl.com/4vb8my7f. She asserts that the "audacious, unprecedented quality" of data collection methods has "impeded our ability to perceive [those methods] and grasp their meaning and consequence." John Laidler, *High Tech Is Watching You*, The Harvard Gazette (Mar. 4, 2019), http://tinyurl.com/5f8swhym.

A big part of the problem, Zuboff believes, is our "dependency and the foreclosure of alternatives." *Id*. Data is collected, as we traverse the Internet, whether we like it or not. In the words of another writer, it is "the dark design patterns"—subtle opt-ins, fine print in terms of service, etc.—that supposedly "force us to opt in to data collection." Ben Lee, *Putting the 'Capitalism' in 'Surveillance Capitalism'*, Current Affairs (May 15, 2021), http://tinyurl.com/2fd7ydwu. Even when users are aware of data collection, they sometimes, in Zuboff's view, simply have no choice but to divulge information in order to use the Internet. "We see people who can't afford privacy," she declares—a situation she describes as "profoundly intolerable." Jackson, supra.

Zuboff and the others were not talking about AB 2273's age estimation requirement, but they easily could have been. Age estimation

requires identifying information, such as a user's government-issued ID or a biometric scan of a user's face. See ARB 48-50. An age estimation requirement thus pressures users into allowing invasive data collection. Under AB 2273, the data will be collected whether the users like it or not. Indeed, when age estimation is required by law, users cannot "afford privacy"—when data collection is mandated by the government, privacy cannot be purchased at any price. If data collection really amounts to "the extractive mining of our bodies," Lee, supra, then AB 2273 is an outrage.

Voices on the left (loosely speaking) warn not only about the loss of privacy in general, but also about the loss of anonymity, specifically. "In a democratic society, the ability to speak anonymously … enables free expression without the threat of coercion or retaliation." Riana Pfefferkorn, *Don't Put Anonymous Speech on the Chopping Block*, Boston Review (May 15, 2019), http://tinyurl.com/ycyej8t6. This makes age verification a huge problem. For "age verification systems" are "surveillance systems." Jason Kelley & Adam Schwartz, *Age Verification Mandates Would Undermine Anonymity Online*, Electronic Frontier Foundation (Mar. 10, 2023), http://tinyurl.com/bdhd5uv5. Once a website visitor uploads an ID, or submits to a facial scan, to verify her age, the possibility arises that that information will be retained, shared, sold, hacked, or otherwise abused. *Id.* The notorious Cambridge Analytica

scandal, for instance, involved a "data analytics firm" that "used personal information taken *without authorization*." Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, Guardian (Mar. 17, 2018), http://tinyurl.com/5au34btx. "Every age verification method," users are warned, suffers from these "flaws." Kelley & Schwartz, supra.

For society to enjoy the benefits of online anonymous speech, speakers must "believe the system's assurance of anonymity." Pfefferkorn, supra. Yet "the more information a website collects," users are reminded, "the more chances there are" for that information to be "misuse[d] or mishandle[d]." Kelley & Schwartz, supra. Making matters worse, a visitor can have no confidence that she would *ever find out* about such misuse or mishandling. *Id*. (Making matters worse yet, under AB 2273, websites may "contract with third-parties" for age-verification services—thereby dispersing responsibility for data protection, often to parties unknown to users. AOB 38.) "As much as anything," users are told, "being more anonymous online is linked to your mentality. Simply put, the less you share about yourself online, the less identifiable you will be." Matt Burgess, *How to Be More Anonymous Online*, Wired (Jan. 5, 2024), http://tinyurl.com/2s3p4b3f. AB 2273 prevents users from following that common-sense advice.

Some on the left claim that online surveillance is the product of "massive systematic complicity." Lee, supra. In a sense, that is plainly true—as this case shows. In enacting AB 2273, California has indeed "turn[ed] a blind eye" to its "own complicity" in the erosion of online privacy. *Id*. Nonetheless, many Internet users will make the connection that California has missed. They will see that AB 2273's age-estimation requirement is exactly the kind of surveillance-promoting, anonymity-destroying device that leftwing commentators warn about. These users will sometimes avoid entering, reading, or speaking at websites that require age estimation as the price of entry. AB 2273 would, if implemented, have a chilling effect on these users' speech, in violation of the First Amendment.

II. AB 2273's Age Estimation Provision Will Chill Rightwing Speech.

Oppressive regimes often surveil their citizens' online activity and outlaw online anonymity. See, e.g., Richard Stone, *Iran's Researchers Increasingly Isolated as Government Prepares to Wall Off Internet*, Science (Sept. 11, 2023), http://tinyurl.com/2aup794r; *Vietnam to Crack Down on Anonymous Social Media Accounts*, BBC News (May 9, 2023), http://tinyurl.com/yp3jkbne; Kunwar Shahid, *Pakistan's Missing Activists and the State's War on Online Anonymity*, The Diplomat (Jan.

18, 2017), http://tinyurl.com/w2pf5mcw. A prime offender, in this regard, is the Chinese Communist Party. Notoriously, it is using online surveillance to help it build a "'social credit system' that monitors its citizens' behavior and ranks their trustworthiness." Jeff Kosseff, *The United States of Anonymous* 171 (Cornell Univ. Press 2022). See, e.g., Corbin K. Barthold, *Social Credit: Could It Happen Here?*, City Journal (Autumn 2022), http://tinyurl.com/23uv8czd; Damon Linker, *The Plausible Dystopia of a Social Credit System*, The Week (Feb. 17, 2022), http://tinyurl.com/mr3h9vp8; Samm Sacks & Paul Triolo, *Shrinking Anonymity in Chinese Cyberspace*, Lawfare (Sept. 25, 2017), http://tinyurl.com/3sst8m2a.

Commentators on the ideological right warn of the emergence of a Chinese-style social credit system in the United States. See, e.g., Elle Purnell, *To Punish Putin, U.S. Firms Develop Social Credit System that Would Make Him Proud*, The Federalist (Mar. 8, 2022), http://tinyurl.com/2s39nsfw; Kristin Tate, *Coming Soon: America's Own Social Credit System*, The Hill (Aug. 3, 2021), http://tinyurl.com/pkk7uvfc; Rod Dreher, *Woke Capitalism's US Social Credit System*, The American Conservative (Nov. 9, 2020), http://tinyurl.com/2m7s9zwj. Picking up on this concern, conservative state legislators have introduced bills—some already enacted into law—that bar their states from creating, using, or

supporting a social credit system. See, e.g., Bryan Schott, *Could China's 'Social Credit Score' Happen Here? Utah Lawmakers Move to Make Sure It Can't*, Salt Lake Tribune (Feb. 15, 2023) http://tinyurl.com/4xftmjty; Jimmy Orr, *Wyoming Legislators Fight Back Against Banks Regulating Behavior Through 'Social Credit Scores'*, Cowboy State Daily (July 12, 2022), http://tinyurl.com/3zx3pnev.

Those who see a system of technology-backed social control taking shape in America point to, among other things, the advance of facial-recognition technology, the rise of biometric data collection, and instances of "de-banking" (i.e., shutting targeted individuals out of electronic finance). See, e.g., Samuel Gregg, *Debunking De-banking*, City Journal (Aug. 20, 2023), http://tinyurl.com/2u2d8ud9; N.S. Lyons, *The West and China Share the Same Fate*, UnHerd (Aug. 9, 2023) http://tinyurl.com/f35ed47v. Although these elements might seem to touch on distinct aspects of people's lives, what they ultimately seek to control (the commentators claim) is speech. See, e.g., Linker, supra ("Facial recognition software … can identify individuals attending 'dangerous' protests and other public events."); Lyons, supra ("Debanking … serves as an extremely effective means to isolate and silence a targeted person or group, quickly breaking any presence or influence they may have once had within society.").

Unsurprisingly, therefore, many on the right believe that the keystone of the (supposedly) emerging American social credit system is surveillance and control of online speech. According to Kara Frederick, director of tech policy at the Heritage Foundation, for instance, social media platforms "monitor viewpoints to see whether they conform to leftist politicians' version of reality." Kara Frederick, *Sleepwalking into a China-Style Social Credit System*, The Heritage Foundation (Mar. 4, 2022), http://tinyurl.com/3y64wcja. Frederick asserts "an ideological symbiosis between tech incumbents and government officials," and contends that we're heading toward "tech-enabled totalitarianism." *Id.* Rightwing commentators expose their readers to a steady drumbeat of these warnings. See, e.g., Tyler O'Neil, *Judge Blocks Biden Admin's 'Orwellian' Collusion with Big Tech to Suppress Free Speech*, The Daily Signal (July 11, 2023), http://tinyurl.com/mvz9zsb6; Jonathan Turley, *How the Biden Administration has Quietly Helped to 'Score' Conservative Speech*, The Hill (Feb. 18, 2023), http://tinyurl.com/mt4eddmf; John Kennedy, *Gov. DeSantis Says 'Big Tech' Looks Like 'Big Brother'*, Sarasota Herald-Tribune (Feb. 2, 2021) http://tinyurl.com/4vv3bz32; Frank Miele, *Big Tech, Big Brother, and the End of Free Speech*, RealClearPolitics (Jan 18, 2021), http://tinyurl.com/yc3mps9d.

Conservative Internet users are told, in short, that a social credit system is taking shape—a system that will soon target them. This form of privacy concern differs (obviously) from the kind of privacy concern liberal Internet users read about. See Sec. I, supra. But the take-home is the same: that users should protect their online anonymity. As "traditional beliefs … become increasingly labelled as 'hate speech,'" conservatives hear, "the ability to be anonymous online is a useful protection." David Taylor, *Banning Online Anonymity Is a Seriously Bad Idea, and Could Jeopardise Our Freedom to Share the Gospel*, Premier Christianity (Oct. 22, 2021), http://tinyurl.com/yww8tfks. "Anonymous accounts allow students and other young right-wingers to do online activism without the 'woke mob' getting them fired or ostracised." Sam Bowman, *Eight Reasons Not to Ban Anonymity Online*, Consumer Surplus (Oct. 19, 2021), http://tinyurl.com/3xht4y3u. Online anonymity can help "Christians continue to express their views without fear of losing their job[s]." Taylor, supra. (When, recently, a Republican presidential candidate floated the idea of curtailing online anonymity, her "stance … drew backlash across conservative social media and [from] some of her GOP presidential rivals." Meg Kinnard, *Nikki Haley Walks Back Her Demand that Social Media Ban Anonymous Posters After Facing GOP Backlash*, AP (Nov. 15, 2023), http://tinyurl.com/44b9t329.)

Even if it doesn't actually fuel the rise of a social credit system, data collection can still bring about "an unhealthy entanglement" between online services and the government. *Wash. Post v. McManus*, 944 F.3d 506, 518 (4th Cir. 2019). When an "industry is heavily regulated by government officials," the government can pressure that industry to snoop on customers, to curtail or deny service to people who misbehave (in the eyes of the state), and to "snitch on [people in order] to stay on the good side of federal agencies." J.D. Tucille, *Did Banks Hand Private Financial Data to the FBI Without Legal Process?*, Reason (Aug. 28, 2023), http://tinyurl.com/55sv4ec3. Many—but especially those who see a social credit system emerging—believe that such pressure is already applied, to great effect, on banks, credit card companies, and social media platforms. See, e.g., *id.*; Lyons, supra. It is naïve, we repeat, to assume that data, once collected, will only be used legally and properly. (California should know. See *Failure of Officials to Follow Policy Caused California Gun Owners' Data Leak*, Guardian (Dec. 1, 2022), http://tinyurl.com/444d294h.) Many rightwing Internet users will, therefore, *expect* websites to misuse age estimation data, either at the direct command of, or in an indirect attempt to appease, the government.

Anyone who heeds the warnings of rightwing commentators will think twice before entering, reading, or speaking at a website that

requires age estimation. AB 2273 would, if implemented, have a chilling effect on these users' Internet speech, in violation of the First Amendment.

CONCLUSION

The district court's order granting a preliminary injunction should be affirmed.

February 14, 2024

Respectfully submitted,

/s/ Corbin K. Barthold
Corbin K. Barthold
TECHFREEDOM
1500 K Street NW
Washington, DC 20005
(771) 200-4997
cbarthold@techfreedom.org
Attorney for Amicus Curiae TechFreedom

CERTIFICATE OF COMPLIANCE

I certify:

This brief complies with the type-volume limits of Fed R. App. P. 29(a)(5) because it contains 2,900 words, excluding the parts exempted by Fed. R. App. P. 32(f).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced serif typeface, in 14-point font, using Microsoft Office 365.

/s/ Corbin K. Barthold

CERTIFICATE OF SERVICE

On February 14, 2024, a copy of this brief was filed and served on all registered counsel through the Court's CM/ECF system.

/s/ Corbin K. Barthold