Nos. 19-251, 19-255

IN THE

Supreme Court of the United States

AMERICANS FOR PROSPERITY FOUNDATION,
Petitioner,

v.

XAVIER BECERRA, ATTORNEY GENERAL OF CALIFORNIA,
Respondent.

THOMAS MORE LAW CENTER,
Petitioner,

v.

XAVIER BECERRA, ATTORNEY GENERAL OF CALIFORNIA,
Respondent.

ON WRITS OF CERTIORARI TO
THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BRIEF OF *AMICI CURIAE* HISPANIC LEADERSHIP FUND, NATIONAL ASSOCIATION OF HOME BUILDERS, AND NATIONAL FEDERATION OF INDEPENDENT BUSINESS IN SUPPORT OF PETITIONERS

JEFFREY M. HARRIS
Counsel of Record
WILLIAM S. CONSOVOY
TIFFANY H. BATES
CONSOVOY MCCARTHY PLLC
1600 Wilson Boulevard, Suite 700
Arlington, VA 22209
(703) 243-9423
jeff@consovoymccarthy.com

March 1, 2021

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

STATEMENT OF INTEREST[1]

Hispanic Leadership Fund (HLF). HLF is a not-for-profit 501(c)(4) social-welfare organization. HLF is dedicated to strengthening working families by promoting common-sense public policy solutions promoting liberty, opportunity, and prosperity, with a particular interest in issues affecting the Hispanic community. HLF has previously participated in federal cases in challenges to state laws that unconstitutionally restrict nonprofit organizations' speech and expression. *See, e.g., Hispanic Leadership Fund v. Walsh*, 2013 WL 5423855 (N.D.N.Y. 2013).

National Association of Homebuilders (NAHB). NAHB is a Washington, D.C.-based trade association whose mission is to enhance the climate for housing and the building industry. Founded in 1942, NAHB is a federation of more than 700 state and local associations. About one-third of NAHB's approximately 140,000 members are home builders or remodelers; its builder members construct about 80% of all new homes built in the United States. Chief among NAHB's goals are providing and expanding opportunities for all people to have safe, decent, and affordable housing. The remaining members are associates working in closely related fields within the housing industry, such as mortgage finance and

---

[1] Pursuant to this Court's Rule 37.6, counsel for *amici curiae* certifies that this brief was not authored in whole or in part by counsel for any party and that no person or entity other than *amici curiae* or their counsel have made a monetary contribution to the preparation or submission of this brief. The parties have consented to the filing of this brief.

building products and services. NAHB frequently participates as a party litigant and *amicus curiae* to safeguard the constitutional and statutory rights and economic interests of its members and those similarly situated.

National Federation of Independent Business (NFIB). NFIB is the nation's leading small business association, representing members in Washington, D.C. and all 50 state capitals. Founded in 1943 as a nonprofit, nonpartisan organization, NFIB's mission is to promote and protect the rights of its members to own, operate, and grow their businesses. To protect its members' interests, NFIB frequently files *amicus curiae* briefs in cases that threaten to harm small businesses.

Amici have a significant interest in this case because, as nonprofit organizations dedicated to public policy principles, they have serious concerns about the California Attorney General's *de facto* requirement that nonprofit groups make blanket disclosures of politically and commercially sensitive donor information. This sweeping disclosure demand is especially troubling because, over and over, states have been unable or unwilling to keep nonprofit donor information confidential, thereby exposing the donors and members to harassment and economic reprisals, which ultimately discourages them from associating with and supporting nonprofits. The importance of this case to the nonprofit community simply cannot be overstated. The Court should reverse the Ninth Circuit and make clear that the First Amendment continues to protect the right to confidentiality for

members and donors to nonprofit social-welfare organizations.

INTRODUCTION AND SUMMARY OF ARGUMENT

Petitioners Americans for Prosperity Foundation (AFP) and Thomas More Law Center (Thomas More) have thoroughly explained why compelled blanket disclosure of a nonprofit organization's donors violates the First Amendment. *Amici* write to emphasize and amplify two of the reasons why this Court should reverse the decision below.

First, the Ninth Circuit flatly contradicted *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958) and its progeny in applying lesser scrutiny to California's sweeping disclosure requirement. There are important reasons why heightened scrutiny applies to compelled disclosure of nonprofit donors and membership. By revealing supporters of nonprofits—and thereby exposing them to harassment and economic retribution by those individuals and groups who are opposed to their missions—blanket disclosure rules like California's threaten to stifle core speech and association protected by the First Amendment. This Court has consistently held that there is no basis for imposing such costs on social welfare organizations unless the government is able to overcome heightened scrutiny.

Under any level of scrutiny, however, there is a fundamental mismatch between California's blanket disclosure rules and any government interest in preventing fraud by nonprofit groups. As the FBI and many other groups have recognized, the classic type of

fraud by a nonprofit or charity is when a group raises funds from the public under false pretenses about how the money will be spent, and then diverts the funds to other purposes—or into the pockets of those who run the charity. But compelling upfront disclosure of a list of large donors would do exactly nothing to help law enforcement identify charities engaged in such fraud. It is thus unsurprising that, as the district court found, California has virtually never used this donor information in conducting investigations of charities.

Second, if allowed to stand, the Ninth Circuit's decision upholding California's policy would provide a model by which other states will inevitably force similar disclosures of donor and member information of nonprofit associations. This is especially troubling because many documented cases, discussed below, show that this private information is not going to remain confidential. The temptation for state officials to leak this information is especially great when the nonprofit and the state or local officials are on opposite sides of ideological or public policy issues. Data breaches and accidental disclosures, as well as intentional abuse—like doxing—pose great threats to associations and their members and donors for simply engaging in protected political speech.

But member and donor lists are not only sensitive for speech and advocacy purposes—they are also highly sensitive for business and competitive purposes. Associations work tirelessly to cultivate and develop relationships with members and donors, and disclosure of those lists allows other competing organizations to target and solicit members and donors. California's misguided policy thus not only

threatens to chill nonprofits' speech and advocacy but also unveil commercially sensitive information that is kept confidential for important business reasons. The Ninth Circuit's decision flouts basic principles of the First Amendment, threatens to chill core speech and association, and causes significant harm to nonprofits' missions. The decision below should be reversed.

ARGUMENT

I. The Court should apply heightened scrutiny and enjoin California's attempts to compel the blanket disclosure of highly sensitive donor information.

A. Heightened scrutiny must apply to requirements that nonprofit groups disclose their members or donors.

Compelled disclosure of nonprofits' donor or membership information must be subject to a heightened standard of review. History has shown time and again that such disclosures may subject donors or members to harassment, intimidation, or economic retribution—especially when the organization engages in advocacy that is seen as controversial or is contrary to the policy preferences of state officials. That is why this Court, since *NAACP v. Alabama*, has held that disclosure regimes like the one at issue in this litigation must meet heightened scrutiny. The First Amendment concerns that led to that landmark ruling continue to hold true today and "the full protection of *NAACP v. Alabama* [is] warranted in this case." Thomas More App. 125a (Ikuta, J., dissenting from denial of rehearing en banc).

The NAACP was established in the early 20th century as a private-membership nonprofit, with its original mission to advance racial justice for African Americans through activities coordinated from a central office with affiliates across the country. Anita L. Allen, *Associational Privacy and the First Amendment*: NAACP v. Alabama, *Privacy and Data Protection*, 1 Ala. C.R. & C.L. L. Rev. 1, 3-4 (2011). Today, the NAACP is thriving, with more than 2,000 branches and 500,000 members across the nation. *See* NAACP, *History: Nation's Premier Civil Rights Organization*, bit.ly/3qyGzQ1.

The NAACP's early history, however, was fraught with physical attacks, threats, and intimidation by critics of the nonprofit's outspoken condemnation of racist laws and policies. *See* Allen, *supra* at 4 n.28. This was especially true in the 1950s, as at that time, "the public associated the NAACP with bold, even radical, efforts to force an end to legal segregation" both before and after this Court's decision in *Brown v. Board of Education*. *See id.* at 5. Because there was public resistance to integration, there was resistance to the NAACP. *See id.*

Public resistance to integration and the NAACP itself made Alabama desperate to drive the organization from the state. *See id.* The NAACP's mission to eliminate racial discrimination was a threat to the state's desire to maintain racial segregation. Accordingly, Alabama devised a strategy to expel it by relying on the state's foreign corporation qualification law, which required out-of-state corporations to register before transacting business in the state. *See id.* In 1956, Alabama accused the

NAACP, which had been organized in New York, of failing to register as a foreign corporation. *See NAACP*, 357 U.S. at 451. According to Alabama, the NAACP was operating in the state by, among other things, opening a regional office, organizing chapters, recruiting members, soliciting contributions, and providing both financial support and legal aid to African American students attempting to gain admission to the then all-white University of Alabama. *See id.*; *see also* Allen, *supra* at 5-6.

Although many of Alabama's allegations proved to be untrue, the NAACP *had* failed to comply with the state's foreign corporation qualification law. *See id.* Based on this violation, the Alabama Attorney General secured a court order enjoining the NAACP from operating within the state. *See id.* And, despite the NAACP's extraordinary efforts to come into compliance, including tendering all information needed to register, Alabama refused to back down. Instead, it filed a motion seeking the names and addresses of the NAACP's members and agents. *See id.* The state court granted the motion, forcing the NAACP to either disclose its members or face contempt and a hefty fine.

This Court unanimously overturned that order. Specifically, it held that the NAACP had a right to keep the identity of its members confidential, regardless of whether a state business law had been broken. As the Court explained, forcing the NAACP to disclose its membership to state officials:

> is likely to affect adversely the ability of [the NAACP] and its members to pursue their collective effort to foster beliefs

> which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure.

NAACP, 357 U.S. at 462-63.

This Court's assessment of those risks was unquestionably correct. Given the history of violence facing NAACP members, release of their names and addresses would deter—if not outright prevent—individuals from joining or continuing to affiliate with the organization. *See id.* at 461-62. Indeed, "on past occasions revelation of the identity of its rank-and-file members . . . exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." *Id.* at 462.

At bottom, this Court held that Alabama's efforts to probe into the NAACP's membership implicated concerns at the very core of the First Amendment, as "freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech." *Id.* at 460. Because demands for an advocacy organization's membership lists are "substantial restraint[s on] freedom of association," *id.* at 462, they are "subject to the closest scrutiny," *id.* at 461. Courts must accordingly enjoin such demands unless the state can show a "controlling justification" for disclosure, *id.* at 466, *i.e.*, a "compelling" interest. *Id.*

at 463 (quoting *Sweezy v. New Hampshire*, 354 U.S. 234, 265 (1957) (Frankfurter, J., concurring)).

This Court has never deviated from that understanding of the First Amendment's protections for advocacy organizations. In *Bates v. City of Little Rock*, ordinances in two Alabama municipalities required all organizations operating within their borders to supply the city clerk with the names of the groups' members and contributors. *See* 361 U.S. 516, 516-19 (1960). Two local branches of the NAACP refused to comply since it "might lead to their harassment, economic reprisals, and even bodily harm." *Id.* at 520. NAACP officials successfully appealed their conviction and fines. As the Court explained, "public identification of persons in the community as members of the organizations had been followed by harassment and threats of bodily harm," and moreover, "fear of community hostility and economic reprisals that would follow public disclosure of the membership lists had discouraged new members from joining the organizations and induced former members to withdraw." *Id.* at 524. Having failed to adequately justify its regulation beyond its interest in occupation taxation, the ordinances constituted an unconstitutional restraint on the freedom of association. *Id.* at 527.

In *Talley v. California*, a Los Angeles ordinance restricted the distribution of any handbill that did not include the name and address of the person(s) who printed, manufactured, and/or distributed it. *See* 362 U.S. 60, 60 (1960). The handbills urged readers to boycott certain businesses that allegedly did not offer equal employment to minorities. *See id.* at 61. Just

like the Attorney General's purported interest here in preventing "fraud," Los Angeles attempted to justify its ordinance as "providing a way to identify those responsible for fraud, false advertising and libel." *Id.* at 64. But the ordinance was "in no manner so limited," there was no indication of legislative support for that justification, and "fear of reprisal might deter perfectly peaceful discussions of public matters of importance." *Id.* at 65-66; *see also id.* at 66-67 (Harlan, J., concurring). Accordingly, the Court held that the ordinance violated the First Amendment.

In *Shelton v. Tucker*, an Arkansas statute compelled every teacher, as a condition of employment in any state-supported school or college, to file annual affidavits listing every organization to which they had belonged or regularly contributed to within the past five years. *See* 364 U.S. 479, 480 (1960). Given the disclosure law's unlimited scope, in that it required every teacher to disclose every affiliation, the Court held that it was not sufficiently tailored to the state's interest. *See id.* at 488. This Court held that "even though the governmental purpose be legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved." *Id.* Narrow tailoring was vital, the Court explained, because exposing teachers' associations could threaten their employment due to ideologically opposed superiors and the "public pressures upon school boards to discharge teachers who belong to unpopular or minority organizations. . . ." *Id.* at 486-87.

Finally, in *Gibson v. Florida Legislative Investigation Commission*, the president of the Miami

branch of the NAACP was ordered to appear before a committee of the Florida State Legislature that was investigating infiltration of Communists into organizations operating in the field of race relations and to disclose membership records. *See* 372 U.S. 539, 540-41 (1963). This Court held that Florida had to prove that the investigation into the membership lists of the NAACP was likely to help identify subversives associated with the Communist Party. *Id.* at 548. There, too, the Court held that "*an adequate foundation for inquiry must be laid* before proceeding in such a manner as will substantially intrude upon and severely curtail or inhibit . . . protected associational rights." *Id.* at 557 (emphasis added). Having failed to prove a "substantial connection" between its broader investigative goals and the specific investigation of the NAACP, Florida plainly lacked such a foundation. *See id.*

B. California's blanket donor disclosure policy fails any level of constitutional scrutiny

California has similarly failed to provide a compelling, or even *reasonable*, justification for mandating blanket disclosure of nonprofit groups' largest donors. The district court expressly found that "the state did not really need [the donor] information to accomplish its goals." Thomas More App. 109a (Ikuta, J., dissenting from denial of rehearing en banc). That is especially true when it comes to California's assertion that it needs donor information to weed out charities engaged in fraud. It is, of course, true that the "right to remain anonymous may be abused when it shields fraudulent conduct." *McIntyre*

v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995). But it is equally true that "in general, our society accords greater weight to the value of free speech than to the dangers of its misuse." *Id.*

Regardless of the standard of scrutiny, there must always be a "relevant correlation or substantial relation" between the state's "interest and the information required to be disclosed." *Davis v. FEC*, 554 U.S. 724, 744 (2008) (citations omitted). Even assuming California has a legitimate interest in preventing fraud by charitable organizations, there remains a fundamental disconnect between that interest and the donor-disclosure policy at issue here.

The paradigmatic type of charitable fraud involves situations in which a charity raises funds from the public by making false statements about how it plans to spend that money. Instead of using the money to support the ostensible charitable cause, the fraudsters then funnel the money to themselves or their family members or associates. The FBI, for example, warns the public about charity fraud schemes that "seek donations for organizations that do little or no work" where "the money goes to the fake charity's creator." FBI, *Charity and Disaster Fraud*, bit.ly/37GCHVI. The AARP similarly warns about "scammers" who "capitalize on donors' goodwill to line their pockets." AARP, *Charity Scams*, bit.ly/2Mh4Hro.

California's donor-disclosure rule will do exactly nothing to prevent these common types of charitable fraud. The state "may, and does, punish fraud directly. But it cannot seek to punish fraud indirectly by indiscriminately" demanding that nonprofits turn over their member and donor lists "with no necessary

relationship to the danger sought to be prevented." *McIntyre*, 514 U.S. at 357. Indeed, "[o]ne would be hard pressed to think of a better example of the pitfalls of [California's] blunderbuss approach than the facts of the case before us." *Id.*

Here, it is difficult to imagine even a hypothetical scenario in which fraud that would have otherwise gone undetected would have been caught by state officials by reviewing a list of donors. And the list of donors, of course, provides *zero* information that would help identify common fraudulent schemes such as fundraising under false pretenses or diverting funds from charitable purposes to personal use.

Given the profound disconnect between donor lists and the detection of fraud, it is unsurprising that the donor information is essentially useless to any legitimate law enforcement functions. California's officials have *never* used the donor disclosure information to initiate a fraud investigation. *See* Thomas More Br. 36. Indeed, California officials have candidly admitted that the blanket disclosure policy is not aimed at targeting or investigating fraud. *See* AFP Br. 36-37. At trial, the state's investigative attorneys could not identify a single time they had used a Schedule B in the last year in order to conduct an investigation. *Id.* Not only does the disclosure policy fail to relate substantially to California's interest in detecting fraud, but it fails to relate to that alleged interest *at all*.

NAACP v. Alabama and its progeny make clear that whatever authority state and local governments have to demand information from nonprofits doing business in their respective jurisdictions, they may not

demand disclosure of member and donor information without meeting heightened First Amendment scrutiny. "Individuals who join forces with others" should thus be able "to sleep comfortably knowing they have a constitutional right to privacy that minimizes the risk of stigma or reprisal flowing from group membership." Allen, *supra* at 3. "Any peaceful religious, social, or political organization with a sensitive or unpopular mission," in turn, should be able to promise "meaningful confidentiality and anonymity" to its members and donors. *Id.* After all, "[a]nonymity is a shield from the tyranny of the majority." *McIntyre*, 514 U.S. at 357. Indeed, it "exemplifies" the very "purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society." *Id.* The Court should reverse the decision below to ensure that nonprofit groups are not forced to make blanket disclosures of their highly sensitive donor information to state officials who may be hostile to their goals and ideologically opposed to their missions.

II. Any interest in securing nonprofit member or donor information must be weighed against the substantial likelihood that this highly sensitive information will not be kept confidential.

The Ninth Circuit upheld California's donor disclosure requirement because, among other reasons, there is not "a reasonable probability that the plaintiffs' Schedule B information will become public as a result of disclosure to the Attorney General." AFP

App. 34a; Thomas More App. 37a-38a. As Judge Ikuta explained in her dissent from denial of rehearing en banc, however, that conclusion "is contrary to any real-world experience." AFP App. 93a; Thomas More App. 124a. Indeed, the Court need not look beyond the facts of this case to see just how easily sensitive information can end up in the public domain notwithstanding state officials' promises to keep it confidential.

The undisputed record in this case shows that the Attorney General's office was aware of at least 25 to 30 unredacted Schedule Bs—the part of the IRS Form 990 that contains contributor names, addresses, and donation amounts—that were published on California's Registry of Charitable Trusts website. *See* AFP Pet. 8. For example, Planned Parenthood was forced to complain to the Attorney General about this disclosure of "all the names and addresses of hundreds of [its] donors." AFP App. 52a. Moreover, AFP discovered that the Attorney General had uploaded approximately 1,778 confidential Schedule Bs to its public website, hundreds of which had been publicly available for years. AFP App. 52a; Thomas More App. 123a.

But all of this information would have been available to the public even had it not been intentionally disclosed. It turns out that all confidential information filed with the Registrar of Charitable Trusts, which encompasses at least 350,000 documents (including Schedule Bs), was publicly accessible through the Registrar's website. One needed only to type the URL into a web browser, using the URL from known documents on the

Registrar's website, the document number of the Schedule B sought, and trial and error, in order to view the confidential donor information. ER866, ER931-37, 1035-36. Accordingly, the California Charitable Trusts Section failed to comply with the IRS's requirements for electronic storage, which required the state to set rigorous confidentiality protocols. ER0691-93.

These circumstances led the district court to find that there was a "pervasive, recurring pattern of uncontained Schedule B disclosures—a pattern that has persisted even during this trial." AFP App. 52a; Thomas More App. 62a ("given the history of the Registry completely violating the "longstanding confidentiality policy," the Attorney General's assurances that a regulatory codification of the same exact policy will prevent future inadvertent disclosures rings hollow." . . . "trial testimony supported what should be an obvious fact, the Registry cannot assure that documents will not be inadvertently disclosed no matter what steps it takes.").

Unfortunately, these intentional and unintentional disclosures and sloppy data management practices are not unique to California or this litigation. Improper release of sensitive data has inevitably followed nearly every kind of government information-collection initiative. A 2015 RAND Corporation study found that "data breaches and the unintentional disclosure of personally identifiable information (PII) stemming from loss or theft of digital or printed information were reportedly the most common type of cyber event and, aside from an

individual's name and/or address, credit card numbers and medical information were the most vulnerable types of information." Adrejia L.A. Boutté Swafford, *Cyber Risk Insurance: Law Firms Need It, Too,* 67 La. B.J. 326, 327 (2020). And "[m]alicious intentional attacks far outnumbered those of an accidental basis, totaling around 60% of all incidents." *Id.* (quotations omitted).

As discussed in detail below, breaches have occurred at every level of government, from federal to municipal, and in every setting imaginable. Some include supposedly involuntary releases such as hacking or theft by other means. Other times, the government releases private information intentionally, through leaks, sharing data with third party vendors, and in response to public records requests. As the examples discussed below highlight, this Court should have no confidence in the Ninth Circuit's conclusion that these (or any other) state officials can or will keep this nonprofit membership and donor information confidential.

A. Data breaches, accidental disclosures, and leaks of sensitive information occur regularly at all levels of government.

Data breaches, accidental disclosures, and leaks by government officials occur with unfortunate regularity. Only a few years ago, there was an incident perfectly illustrating the concerns presented by this case. In 2013, the National Organization for Marriage (NOM), whose mission is to "provide educational outreach and to protect marriage as the union of husband and wife and the natural family that springs therefrom as well as the rights of the faith traditions

that support and sustain this marriage culture," sued the IRS for illegally disclosing the confidential part of NOM's Schedule B. *Nat'l Org. for Marriage, Inc. v. United State*s, 24 F. Supp. 3d 518 (E.D. VA. 2014); Peter Reilly, *National Organization for Marriage Denied Attorney Fees in IRS Lawsuit*, Forbes (Dec. 9, 2015), bit.ly/3qVgF9c. The information had been illegally provided to an activist, who turned it over to the Human Rights Campaign, which in turn provided it to the Huffington Post. *See* Reilly*, supra.* The IRS admitted the wrongdoing and settled the lawsuit. *See id.* But that hardly remedied all of the harm resulting from the disclosure. The strategic leak forced a CEO to step down from a prominent software company as a result of public pressure once his contribution to the group had been made public. *See id.*

In October 2018, a government computer system that interacts with HealthCare.gov was hacked, compromising the sensitive personal data of approximately 75,000 people. Richard Alonso Zaldivar, *Hackers Breach HealthCare.gov System, Get Data on 75,000*, Associated Press (Oct. 19, 2018), bit.ly/2m0DsEa. HealthCare.gov collects an array of information from individuals applying for subsidized health insurance, including their names, social security numbers, family information, income, and citizenship or immigration status. *See id.* Concerningly, it appears that officials waited to inform consumers that their information may have been compromised until a time that was favorable from a public relations standpoint. *See id.* The hack and data breach forced officials to shut down the affected portion of the website, and to offer credit protection to some victims. *See id.*

In late 2018, Indian cybersecurity firm Banbreach discovered that a server hosting the California Department of Insurance (CDI) website had seen a large uptick in generation of reports, indicating a vulnerability and thus the potential exposure of personal information. *California Department of Insurance Vulnerability Potentially Exposed Thousands of SSN and Other Personal Information*, DataBreaches.net (Jan. 5, 2019), bit.ly/2ksfJw0. In particular, the server generated more than 24,450 reports in 24 hours. *See id.* These reports included renewal reports for insurance agents that included the agents' name, renewal ID, and Tax Identification Number (TIN), but because many individuals use their social security number as their TIN, it is certain that many people had their names and social security numbers compromised. *See id.* Other reports were potentially exposed, too, including insurance claims and investigation reports with details such as names, vehicle registration numbers, and addresses; statistical reports on monthly frauds; and details of individuals and the charges they were indicted for, the fines they paid, and the parties harmed by their alleged malfeasance. *See id.* It appears that the CDI still has not notified any of the potential victims or made an announcement on a state website about this serious breach. *See id.*

In February 2018, an employee at Oregon's tax collection agency copied the data of 36,000 people (including social security numbers) and saved the data to a personal account. Hillary Borrud, *Oregon Tax Agency Employee Copied Personal Data of 36,000 People*, The Oregonian (Mar. 23, 2018), bit.ly/2kZ7Xdd. The data breach included files that

were related to a list of taxpayers who paid their taxes using checks and turned out to have insufficient funds. *See id.* Oregon officials waited a month to disclose the breach. *See id.*

In late 2018, the Missouri Department of Health and Senior Services discovered a data breach implicating the personal information of over 10,000 people. *Announcement from the Missouri Department of Health and Senior Services*, Missouri Dep't of Health & Senior Servs. (Oct. 26, 2018), bit.ly/2m8bXbv. Apparently, an information technology contractor, who had worked on a Department information system, improperly retained the personal information and then allowed it to be stored in an electronic file that was not password-protected. *See id.* This information included names, dates of birth, identification numbers issued by State agencies, and social security numbers. *See id.*

Earlier that year, it was discovered that an employee of the Veteran Affairs Medical Center in Long Beach, California had stolen the health information of more than 1,000 patients. *3-Year Jail Term for VA Employee Who Stole Patient Data*, HIPPA Journal (Jun. 18, 2018), bit.ly/2ktIkkz. The breach was discovered when the perpetrator was stopped by police officers, who uncovered in his vehicle prescription medications for which he did not have a prescription and the Social Security numbers and other health information pertaining to fourteen patients. *See id.* A search of his apartment revealed hard drives and zip drives containing the private health information of 1,030 patients. *See id.*

In 2019, two computers that were being used in an Atlanta-area school board election were stolen from a precinct. Mark Niesse & Arielle Kass, *Check-in Computers Stolen in Atlanta Hold Statewide Voter Data*, Atlanta News Now (Sep. 17, 2019), bit.ly/2m0Exfc. These computers contained Georgia's statewide voter information—including the "names, addresses, birth dates and driver's license information for every voter in the state." *Id.*

In August 2011, confidential documents from the Louisiana Department of Children and Family Services, which include personal information, were found blowing down the street before being collected and turned over to a local TV station. *Confidential Louisiana Department of Children and Family Services Documents Found Blowing in the Street; Office Manager and Area Director Suspended*, DataBreaches.net (Aug. 22, 2011), bit.ly/2NC2YgP. A large trash bag filled with copies of dozens of social security cards, bank records, birth certificates, and other confidential documents was similarly discovered by a passerby on a downtown Baton Rouge street. *See id.* The paperwork appeared to be connected to applicants for various forms of public assistance such as food stamps, welfare, and childcare assistance cases. *See id.* Two state employees with the Department of Children and Family Services were suspended when it was discovered that the documents were improperly discarded in a trash can accessible to the public. *See id.*

In a 2012 incident, the California Department of Child Support Services lost a staggering amount of sensitive personal data. GoBankingRates, *California*

Doesn't Know What it Did with 800,000 Child Support Records, Business Insider (Apr. 3, 2012), bit.ly/3bHwKsT. As part of a disaster preparedness exercise, the agency transferred to an IBM facility in Colorado information necessary to operate California's child support system remotely in the event of a disaster. *See id.* After the exercise was deemed successful, the files were to be transported back to the Department via a transportation contractor. *See id.* Before the files reached their destination, however, four computer storage devices containing, among other things, social security numbers, names, addresses, driver's license numbers, and names of health insurance providers for about 800,000 people, went missing. California recommended that those 800,000 people place fraud alerts on their credit cards, obtain credit reports, and take additional steps to monitor their private information. *See id.*

In the Fall of 2018, the Oklahoma Department of Human Services inadvertently sent letters meant for people with developmental disabilities to incorrect addresses. Dale Denwalt, *Oklahoma DHS Could Have Sent Private Medical Info to Wrong Addresses*, The Oklahoman (Oct. 2, 2018), bit.ly/2kWrUS3. The letters informed patients and their guardians about changes to their plan of care, but also included personal information. *See id.* Apparently, the error was caused by a computer that labeled envelopes incorrectly and affected at least 800 people. *See id.*

These examples—which are surely just the tip of the iceberg given that they necessarily involve only *detected* data leaks or breaches—underscore the dangers inherent in government data collection and

the serious risks of intentional or unintentional disclosures of sensitive information even when officials exercise far more care than the California officials did here. This Court should thus give little, if any, weight to Respondents' promises to keep donor information "confidential," as there remain serious risks that this information will ultimately end up in the public domain.

B. Countless individuals have faced harassment, threats, and loss of business opportunities after being "doxed" for engaging in core political speech.

Not only are there countless instances of sensitive and confidential information being released each year, but an increasing number of them result in job losses, threats, intimidation, and even violence. Especially when an individual or group advances positions that are seen as unpopular or controversial, it has become all too common for those affiliated with the group or the speaker to face both personal and professional intimidation and reprisals.

Unfortunately, "[o]ver the past few years, doxing—publishing private information about people online, generally with the intent of threatening them—has become part of the underbelly of politics." Rachel Kurzius, *Why Do These Activists Publish People's Addresses but Fear the Same Treatment?*, Wash. Post (Jan. 9, 2019), wapo.st/3dtWwDi. For example, in 2019, an activist group, Smash Racism DC, published Fox News host Tucker Carlson's home address on Twitter. More than a dozen activists showed up at Carlson's house, harassing his wife and four children inside and chanting "We know where you

sleep at night!" *Id.* When interviewed, one of the protestors outside Carlson's house admitted that doxing is "designed to make you feel on edge." *Id.*

In 2018, then-Senator Orin Hatch and Senators Mitch McConnell, Lindsay Graham, Mike Lee, and Rand Paul suffered threats and harassment after a former aide to Senator Maggie Hassan hacked Senate computers and released the Senators' personal information, including their home addresses and phone numbers. Josh Gerstein, *Ex-Hassan Aide Sentenced to 4 Years for Doxing Senator*s, Politico (June 19, 2019), politi.co/3uilqvN. In what is considered "the largest data breach in Senate history," the former aide "cop[ied] dozens of gigabytes of sensitive data, and install[ed] sophisticated keyloggers that captured the work and personal computer passwords of [Senate] staffers as they logged in." *Id.* The former aide doxed the Senators "solely because 'they had different political opinions from'" him. And the judge who sentenced the aide to prison specifically noted that "criminal harassment driven by political motives" is an increasing problem in our "very vicious" society." *Id.*

The "doxing" problem has also spread to college campuses. In 2019, a student group called the Autonomous Student Network threated to dox students at the University of Texas-Austin who joined conservative student organizations. *See* Jon Street, *Incoming Texas Freshmen Threatened with Doxing if They Join Conservative Campus Groups*, Campus Reform (June 21, 2019), bit.ly/3k7NPjy. They announced to the incoming freshman class on Twitter, "If you join YCT [Young Conservatives of Texas] or

Turning Point USA ... Your name and more could end up on an article like one of these," tweeting a website listing previously posted email addresses and phone numbers of students who had shown support for a Supreme Court nominee. *Id.*

Some individuals also face job losses for expressing unpopular beliefs or supporting certain organizations. For example, Facebook fired former executive Palmer Luckey, known as "a rising star of Silicon Valley," after it was revealed that Mr. Luckey donated money to "an anti-Hillary Clinton group." Kirsten Grind & Keach Hagey, *Why Did Facebook Fire a Top Executive? Hint: It Had Something to Do with Trump*, Wall St. J. (Nov. 11, 2018), on.wsj.com/2NJChGM. And just this year, Cara Dumaplin, creator of a popular infant sleep training program faced harassment and boycotts after activists revealed that she had donated to President Trump. Activists also threatened to illegally disperse her sleep training materials. Rheana Murray, *Moms Boycott Popular Baby Sleep Expert for Donating to Trump*, Today (Jan. 21, 2021), on.today.com/2OM88am.

In sum, it is now easier than ever for malicious actors to *obtain* personal information, and there is also more opportunity than ever to *use* that information to engage in harassment, intimidation, or blacklisting. The risks of disclosures and the serious consequences of such disclosures must accordingly be considered prominently in any analysis of the important First Amendment interests at stake here.

C. Nonprofit organizations' donor and membership information is also highly commercially sensitive.

Finally, donor and membership lists are not only sensitive for advocacy and First Amendment purposes, but they are also extremely sensitive for business and competitive purposes. It is well-understood in the nonprofit community that the "cultivation and acquisition of lists" is "[c]rucial to the marketing success of . . . nonprofit organizations." Ely R. Levy, *Nonprofit Fundraising and Consumer Protection: A Donor's Right to Privacy*, 15 Stan. L. & Pol'y Rev. 519, 528 (2004). "Obtaining, refining, and exploiting lists has become an economic consideration relevant to nearly every company[]" in America. *Id.* Indeed, donor lists even "usually qualify as depreciable assets for tax and accounting purposes." *Id.* at 528.

Allowing broad access to confidential donor or membership lists—as California's blanket disclosure policy will inevitably do—gives an organization's competitors the opportunity to take advantage of that hard-earned information for their own business gain, including by using those lists to solicit another organization's donors or members. And there will surely be third-party data vendors willing to trade in any information that is disclosed. This is an especially important consideration given that "[t]rading in personal information about consumers and donors has become pattern and practice" and "'[d]ata-mining' has become more valuable, in all respects, than ever." *Id.* at 526-27. Some observers have even contended that "when one gives a donation to a charity, the name and

personal information that comes with the donation is more valuable than the donation itself." *Id.* at 530.

Like countless other nonprofit groups, *amici* invest significant time and resources in building goodwill among their members and donors and ensuring that those stakeholders remain committed to each organization's mission. In addition to burdens on speech and association protected by the First Amendment, allowing the Ninth Circuit's decision to stand would also diminish the value of nonprofit organizations' hard-earned base of donors and members. The commercial and economic implications of the decision below are as profound as the consequences for speech and expression, and all relevant considerations point in the same direction: California's policy and the Ninth Circuit's decision are untenable.

CONCLUSION

For the foregoing reasons, the Court should reverse the decision below.

Respectfully submitted,

JEFFREY M. HARRIS
Counsel of Record
WILLIAM S. CONSOVOY
TIFFANY H. BATES
CONSOVOY MCCARTHY PLLC
1600 Wilson Boulevard, Suite 700
Arlington, VA 22209
(703) 243-9423
jeff@consovoymccarthy.com

March 1, 2021 *Counsel for Amici Curiae*