No. 19-251, No. 19-255

In The
Supreme Court of the United States

AMERICANS FOR PROSPERITY FOUNDATION,
Petitioner,
v.
XAVIER BECERRA IN HIS OFFICIAL CAPACITY AS THE ATTORNEY GENERAL OF CALIFORNIA,
Respondent.

THOMAS MORE LAW CENTER,
Petitioner
v.
XAVIER BECERRA IN HIS OFFICIAL CAPACITY AS THE ATTORNEY GENERAL OF CALIFORNIA,
Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

BRIEF *AMICUS CURIAE* OF THE HISPANIC LEADERSHIP FUND IN SUPPORT OF PETITIONERS

JASON TORCHINSKY
DENNIS W. POLIO
HOLTZMAN VOGEL
JOSEFIAK TORCHINSKY PLLC
North Hill Drive, Suite 100
Warrenton, VA 20186
(540) 341-8808

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

Attorneys for Amicus Curiae

September 25, 2019

LANTAGNE LEGAL PRINTING
801 East Main Street Suite 100 Richmond VA 23219 (800) 847-0477

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

Amicus curiae the Hispanic Leadership Fund (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 been a participant in federal cases in order to advance its social-welfare mission. *See, e.g.*, *Hispanic Leadership Fund v. Walsh*, 2013 WL 5423855 (N.D.N.Y. 2013).

HLF is interested in this case because, as a not-for-profit organization dedicated to public policy principles, it is distressed by the California Attorney General's *de facto* requirement that all nonprofit groups turn over sensitive donor information. This sweeping and unjustified disclosure demand is especially disturbing to HLF because, over and over, States have proven their inability to keep nonprofit information confidential, thereby exposing the donors and members to violence, harassment, and economic reprisals, which ultimately discourages them from associating with nonprofits. HLF especially feels this impact given the organization's focus on issues affecting minority communities. The importance of this case to HLF and other nonprofits simply cannot be overstated.

---

[1] Pursuant to this Court's Rule 37.6, counsel for *amicus 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 *amicus curiae*, its members, or its counsel has made a monetary contribution to the preparation or submission of this brief. The parties have consented to the filing of this brief.

This case is not about public disclosure of information related to elections or ballot measures. Rather, it is about how much disclosure States may demand from nearly any organization operating within their respective borders. The Court should grant review, reverse the Ninth Circuit, and make clear that the First Amendment continues to protect the right to anonymity for members of—and donors to—nonprofit social-welfare organizations.

INTRODUCTION & SUMMARY OF THE ARGUMENT

Petitioners Americans for Prosperity (AFP) and Thomas More Law Center (Thomas More) have thoroughly explained why the Court should decide this important First Amendment question that has divided the lower courts. *Amicus curiae* submits this brief to emphasize and amplify two of the reasons why this Court's review is so urgently needed and review should be granted.

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 violence, harassment, and economic retribution by those individuals and groups who are opposed to their missions, disclosure threatens to stifle First Amendment protected speech and association. Supporters will inevitably cease associating—or

decline to associate—with nonprofits in the first place, if the costs of doing so are this high. 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.

Second, the Ninth Circuit has provided a pathway by which other States will inevitably force similar disclosure of donor and member information, as well as the disclosure of other confidential information about the inner workings of nonprofit associations. This is especially troubling because experience shows that this private information is not going to remain confidential. The temptation for state officials to leak this information is great when the nonprofit and the state or local officials are on opposite sides of ideological divide and/or public policy issues. But data breaches and accidental disclosures pose as perhaps greater threats than intentional abuse. Before this information is disclosed, the government should have to prove it has a compelling need for the information. California cannot even come close to making that showing. The Court should grant certiorari.

ARGUMENT

I. HEIGHTENED SCRUTINY MUST APPLY TO NONPROFIT DISCLOSURE REQUIREMENTS.

Compelled disclosure of nonprofit information must be subject to a heightened standard of review. The personal information of donors and members is especially sensitive. History proves that disclosure

exposes them to violence, harassment, and economic retribution. The potential for this type of intimidation, naturally, increases exponentially when the nonprofit espouses controversial views on matters of public concern that are unpopular with 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 the seminal ruling in *NAACP v. Alabama* continue to hold true today and necessitate the Court's intervention.

The NAACP was established in the early Twentieth Century as a private-membership non-profit, 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, at 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*, https://www.naacp.org/nations-premier-civil-rights/organization/.

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 corporate 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 overturned that order. Specifically, it held that the NAACP had a right to keep the identity of its members secret, regardless of whether a state business law had been broken. As the Court unanimously held, revealing the members:

> 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.

The Court's assessment was no doubt 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, "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 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 strike down 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)).

The Court has not deviated from this understanding. 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 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 (1960). The handbills urged readers to boycott certain businesses that allegedly did not offer equal employment to minorities. *See id.* at 61. Los Angeles attempted to justify the 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 5 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*. Fit 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.

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. Here 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. Having failed to prove a "substantial connection" between its broader investigative goals and the specific investigation of the NAACP, Florida lacked such a foundation. *See id*.

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.[2] "Individuals who join forces with others" thus should 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*.

Unfortunately, that will not be the case if the Ninth Circuit's ruling is not overturned. The decision provides a roadmap for any state official to demand donor information from nonprofits with whom they ideologically disagree. This is not an abstract

---

[2] This is distinct from the public disclosure that the Court has approved in the campaign finance context. In campaign finance, public disclosure of political donors has been seen as the "least restrictive means of curbing the evils of campaign ignorance and corruption." *Buckley v. Valeo*, 424 U.S. 1, 68 (1976) (per curiam). But those concerns are not present here. Americans for Prosperity Foundation and the Thomas More Law Center operate under Section 501(c)(3) of the Internal Revenue Code. As such, they are effectively prohibited from engaging in political activity. *Regan v. Taxation with Representation of Wash.*, 461 U.S. 540 (1983). Like the NAACP, these are groups of individuals associating together to further social-welfare goals. As a consequence, a stricter standard must apply.

concern. Today, many nonprofits face State government officials that are ideologically opposed to their missions and committed to disclosing the names of their donors and members. Allowing this to happen will expose donors and members to violence, harassment, and economic retribution. For Americans for Prosperity and the Thomas More Law Center, as their certiorari petitions recount, it already has.

II. ANY INTEREST IN SECURING NONPROFIT MEMBER AND DONOR INFORMATION MUST BE WEIGHED AGAINST THE LIKELIHOOD THAT THIS SENSITIVE INFORMATION WILL NOT BE KEPT CONFIDENTIAL.

The Ninth Circuit upheld the 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 that Judge Ikuta is right.

As Petitioners explain, 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. In fact, Planned Parenthood was forced to complain to the Attorney General about this disclosure of "all the names and addresses of hundreds of [its] donors." Moreover, AFP discovered that the Attorney General had uploaded approximately 1,778 confidential Schedule Bs on 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 publicly available 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.

All of this 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."). But none of this is unique to California or this litigation. Improper release of sensitive data has followed nearly every kind of government information-collection initiative. Breaches have occurred on 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 representative examples included below highlight, the Court should have no confidence in the Ninth Circuit's conclusion that this (or any other) Attorney General can or will keep this nonprofit member and donor information confidential.

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. *National Org. for Marriage, Inc. v. United States*, 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), https://www.forbes.com/sites/peterjreilly/2015/12/09/national-organization-for-marriage-denied-attorney-fees-in-irs-lawsuit/#5ee8a9123f60. The information had been provided to a gay rights activist, who turned it over to the Human Rights Campaign (HRC), which in turn provided it to the Huffington Post. *See id*. The IRS admitted the wrongdoing and settled the lawsuit. *See id*. But that did not remedy all of the harm. The strategic leak forced a CEO to step down from a prominent software company due to his now-public contribution to this pro-life group. *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), http://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 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), http://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 possible that many people had their name and social security number 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 has not notified any of the potential victims or made an announcement on a state website about this issue. *See id*.

In February 2019, 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),

http://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 Department of Health and Senior Services (Oct. 26, 2018), http://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 this 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), http://bit.ly/2ktIkkz. The breach was discovered when the perpetrator was stopped by police officers and 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

uncovered hard drives and zip drives containing the private health information of 1,030 patients. *See id.*

Just last week, two computers that were being used in an Atlanta-area school board election were stolen from a precinct. Mark Niesse and Arielle Kass, *Check-in Computers Stolen in Atlanta Hold Statewide Voter Data*, Atlanta News Now (Sep. 17, 2019), http://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), https://www.databreaches.net/confidential-louisiana-department-of-children-and-family-services-documents-found-blowing-in-the-street-office-manager-and-area-director-suspended/. 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), http://bit.ly/2kpZIGS. 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), http://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.*

In all, these examples demonstrate the dangers inherent in government data collection and the need for heightened review here. When organizations like AFP and Thomas More are forced to disclose their member and donor list to state and local officials opposed to the ideological mission of these nonprofits, the potential for abuse multiplies. Before such sensitive information is disclosed, the government should be required to establish a compelling need for it—something the California Attorney General has plainly failed to do here.

CONCLUSION

Amicus curiae respectfully requests that the Court grant the petition for certiorari.

Respectfully submitted,

JASON TORCHINSKY
DENNIS W. POLIO
HOLTZMAN VOGEL
JOSEFIAK TORCHINSKY PLLC
North Hill Drive, Suite 100
Warrenton, VA 20186
(540) 341-8808

JEFFREY M. HARRIS
WILLIAM S. CONSOVOY
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd, Suite 700
Arlington, VA 22209
(703) 243-9423
jeff@consovoymccarthy.com

September 25, 2019

Attorneys for Amicus Curiae