Nos. 19-251, 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 WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

BRIEF FOR CHINA AID ASSOCIATION AS *AMICUS CURIAE* IN SUPPORT OF PETITIONERS

SEAN P. GATES
Charis Lex P.C.
301 N. Lake Ave.
Ste. 1100
Pasadena, CA 91101
(626) 508-1715
sgates@charislex.com

ANDREW C. NICHOLS
Counsel of Record
Charis Lex P.C.
4250 N. Fairfax Dr.,
Ste. 600
Arlington, VA 22203
(571) 549-2645
anichols@charislex.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTRODUCTION & STATEMENT OF INTEREST[1]

China Aid Association, or, more simply, ChinaAid, is an international nonprofit Christian human rights organization committed to promoting religious freedom and the rule of law in China, as well as supporting Chinese Christians and their families who have experienced persecution at the hands of their government.

ChinaAid was founded nearly 20 years ago by Bob Fu, a student leader in the 1989 Tiananmen Square demonstrations. In 1997, Fu and his family fled to the United States where Fu earned his doctorate. In addition to leading ChinaAid, Fu serves as Editor-in-Chief of *Chinese Law & Religion Monitor*, a journal on religious freedom and the rule of law in China. He has testified before the House Foreign Affairs Committee, the Senate Judiciary Committee, the Congressional-Executive Commission on China, several European parliaments, the parliament of the European Union, and the U.N. Commission on Human Rights. He is also a member of the Council on Foreign Relations.

ChinaAid submits this brief to lend crucial international context to this Court's decision, which will directly affect donors to human-rights groups. Scholars of all stripes agree that we are witnessing an unprecedented era of what they call "transnational repression" by China. Surveillance, harassment, intimidation, abduction of family members, death threats—China uses the entire cross-border toolkit with a skill and ferocity

---

[1] No counsel for any party authored this brief in whole or in part, and no person other than *amicus curiae* and its counsel contributed financially to preparing or submitting this brief. All parties have consented to the filing of this brief.

never seen before. Many of China's targets are dissidents. And they include Bob Fu, who recently had a bounty placed on his head on YouTube and Twitter by an apparent proxy of China living in the United States. Fu's family fled their home and dispersed, and he had to shutter the offices of ChinaAid.

As the statutorily established Congressional-Executive Commission on China put it, China is exhibiting "a toxic blend of Mao's ruthlessness and sophisticated 21st-century surveillance techniques—in effect, an updated religious Cultural Revolution." No government, organization, or individual is secure. Last summer, China hacked into the Vatican. Before that, it cracked the iPhone—and the Android system. And before that, it stole myriad files from the Office of Personnel Management, including 5.6 million sets of fingerprints.

Which brings us to California's blanket mandate that charities disclose their top donors' names and addresses to California, which uploads that information onto the Internet. What could possibly go wrong? The answer, alas, is all too clear on the record here. China's hackers inevitably will exploit the porous registry, and China will go after donors to organizations like ChinaAid as it has gone after Bob Fu.

The Ninth Circuit acknowledged that the State exposed some 1,800 donor lists to the public by accident. But the court drew comfort from California's plan to continue to trust students and temporary workers to upload donor lists only onto the *private* Internet, thanks to new "weekly" checks. Of course, that will still leave the lists exposed for up to six days—plenty of time for China's hackers. But *not* plenty of time for donors to bring an as-applied challenge. The mandate should be struck down in its entirety.

SUMMARY OF ARGUMENT

I. California's blanket donor-disclosure mandate poses serious, needless risks to donors to human-rights groups that criticize nation-states like China. China is the world's leading transnational oppressor—surveilling, harassing, and intimidating critics around the world, including in the United States. China has sent agents into the United States to coerce Chinese exiles to come back to China to stand trial, and it has passed laws asserting global extraterritorial jurisdiction over its critics. China especially targets religious minorities, most recently focusing on Muslims, whom China often coerces into silence by threatening to retaliate against their relatives still in China.

China has acted to harass, threaten, and intimidate ChinaAid, which, along with its supporters, China has labeled "anti-China forces." Recently, China unleashed a proxy in the United States who repeatedly urged his hundreds of thousands of social-media followers to "kill" ChinaAid's founder, Bob Fu, along with another democracy activist in California.

One of China's key means of attacking critics abroad is by hacking into their accounts and organizational systems. Hundreds of entities have been penetrated—from technology firms, to universities, to nonprofits, to religious institutions. Another favorite target is government agencies, including, most notoriously, the U.S. Office of Personnel Management. In past years, China employed primitive techniques, but now shows skills exceeding those of the Federal Bureau of Investigation ("FBI"). Recently, for example, China hacked into the iPhone, when the FBI could not.

II. It is only a matter of time, therefore, before China's sophisticated hackers invade California's low-

tech registry to find the names and addresses of donors to organizations that China views as critics. That is the kind of information China uses to silence people and hobble entities like ChinaAid. Donors will likely stop giving if they believe they or their family in the United States may be threatened with death, as was Bob Fu. This is not to mention donors who have family in China, where China exerts more vicious pressure.

Though the Ninth Circuit did not intend to do so, its decision highlights the vulnerability of California's registry to China's hackers. Even under its new security protocols, California uploads the entire contents of its donor registry—some 60,000 donor lists—to the Internet every year. That "tedious" task is left to the same "temporary" and "student" workers who "inadvertently misclassified as public" some 1,800 donor names and addresses. The State now checks for errors weekly, but that still leaves donor lists exposed for up to six days, when China's hackers will have free rein. For an error to be fixed immediately, a donor must ask.

If there were any doubt that California's registry cannot withstand China's hackers, it was eliminated before trial. During discovery, California was told of a flaw that allowed one of petitioners' experts to see all 350,000 confidential documents in the registry. The State claimed to fix the problem, and the problem of the 1,800 lists mislabeled as public. But the day before trial, the expert found dozens of lists still online. The State will be no match for China if it is no match for petitioners' expert, who effectively spotted the State the time and exact nature of his attack.

III. All of this counsels for overturning California's mandate wholesale. Once donor information is stolen, it will be too late to bring an as-applied challenge.

ARGUMENT

I. California's mandate poses grave risks to donors to human-rights groups like ChinaAid, which is facing extreme repression by China.

The risks posed by California's blunderbuss mandate are felt acutely by nonprofits, like ChinaAid, that face down powerful nation-states for human-rights violations. Increasingly, such nation-states surveil and attack their opponents across borders—in what has become known as "transnational repression." Freedom House, *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression*, at 1 (Feb. 2021) (Transnational Repression Report). All of these nation-states have both the will and sophistication to exploit California's primitive, problem-riddled donor registry. But none compares to China, which is in the midst of a full-throttle attack on ChinaAid in the United States.

A. On an unprecedented scale, China is surveilling, harassing, and intimidating critics globally, including in the United States.

1. China "conducts the most sophisticated, global, and comprehensive campaign of transnational repression in the world." *Id.* at 15. "[T]he sheer breadth and global scale of the campaign is unparalleled." *Ibid.* China conducts a "[b]road[] system of surveillance, harassment, and intimidation that leaves many overseas Chinese and exile minorities feeling that the [Chinese Communist Party] is watching them and constraining their ability to exercise basic rights even when living in a foreign democracy. All told, these tactics affect millions of Chinese and minority populations from China in at least 36 host countries." *Ibid.* Nor is China satisfied with repressing ethnic Chinese

and exiled minorities. "China's attempts to intimidate and control *foreigners* in response to their peaceful advocacy activities is an ominous trend." *Id.* at 16 (emphasis added).

China's "long arm of authoritarianism" extends into the United States. Congressional-Executive Commission on China, *Annual Report* 1 (2020) (Congressional-Executive Commission Report). China's efforts here "include threatening and intimidating critics, blocking social media content, pressuring publishers to censor their content in China, influencing academic institutions to the detriment of academic freedom, interfering in multilateral institutions, and pressuring U.S. and international companies to suppress practices that do not conform to the political narratives and demands of Chinese officials." *Ibid.* And the threat is growing. "[T]he Chinese government and Communist Party have taken unprecedented steps in the last year to extend their repressive policies through censorship, intimidation, and the detention of individuals and groups for exercising their fundamental human rights[.]" *Ibid.*

In one of China's most high-profile moves—which it proudly dubs "Operation Fox Hunt"—China sent agents to the United States "to conduct an aggressive harassment campaign on behalf of China to pressure political dissidents and fugitives in the United States to return home to face trial[.]" Michael Schmidt, *U.S. Charges 8 in Plot to Harass Chinese Dissidents*, N.Y. Times (Oct. 28, 2020). "In 2015, top Obama officials privately warned Chinese officials to stop using their agents in the United States to harass expatriates." *Ibid.* But evidently the warning went unheeded. Eight Chinese agents have now been charged with "carrying out an elaborate pressure campaign that

included hiring American private investigators to locate the expatriates who had taken refuge in the United States and then stalking, surveilling and threatening them and their family members." *Ibid.* "In one instance, the operatives arranged for threatening messages to be sent on social media to the daughter of a former Chinese official and to her friends[.]" *Ibid.* "They also brought the official's father to the United States from China to use the unannounced presence to threaten his son to return home." *Ibid.* (internal quotation marks omitted).

To heighten the threat to its critics, China is now increasingly asserting extraterritorial jurisdiction over anyone, anywhere. In its so-called "National Security Law," which ostensibly tightens China's control over Hong Kong, China also "criminaliz[ed] any speech critical of the Chinese or Hong Kong government *made anywhere in the world, including speech by foreign nationals*." Transnational Repression Report 19-20 (emphasis added). "Among those who received the first round of arrest warrants under the new law was Samuel Chu, an American citizen, who was charged for his work to gain US government support for the cause of freedom in Hong Kong. Chu and others like him now must not only avoid traveling to Hong Kong, but also to any country with an extradition treaty with Hong Kong or China." *Ibid.* Meanwhile, China also "announced plans to sanction 11 U.S. politicians and heads of organizations that further democracy and human rights around the world, including National Endowment for Democracy president Carl Gershman, National Democratic Institute president Derek Mitchell, International Republican Institute president Daniel Twining, and Freedom House president Michael Abramowitz." Freedom House, *Democracy and*

Human Rights Organizations Respond to Threat of Government Sanctions (Aug. 12, 2020).

2. Although no one is safe from China's attacks, some of its most brutal assaults have come against religious minorities. "Chinese believers and outside experts compared the current situation to the Cultural Revolution (1966 to 1976), widely seen as the most repressive era for religions in [People's Republic of China] history." Congressional-Executive Commission Report 11. "[O]ne expert describe[es] the present situation as 'a toxic blend of Mao's ruthlessness and sophisticated 21st-century surveillance techniques—in effect, an updated religious Cultural Revolution.'" *Ibid.* As a Chinese Catholic priest explained, "[i]n practice, your religion no longer matters, [whether] you are Buddhist, or Taoist, or Muslim or Christian: the only religion allowed is faith in the Chinese Communist Party." *Id.* at 112.

In the United States, China's campaign against religious dissidents has recently focused on Muslims. "Identified agents of the Chinese government" have "intimidated and harassed members of China's Turkic Muslim minorities residing in the United States, particularly those from the Uyghur community. In many cases, this harassment included threats to family members still in China * * * *. Uyghurs inside the United States who chose to speak out about worsening persecution of their community by the Chinese government reported retaliation against family members and acquaintances still in China." Congressional-Executive Commission Report 14. "This intimidation and harassment has taken place alongside the mass persecution of Uyghurs within China, backed by pervasive electronic and physical surveillance and widespread reported incidents of arbitrary detention and torture."

Id. at 154. Indeed, the repression in the United States conspicuously accelerated in 2017, "when the Chinese government began constructing a network of mass internment camps * * * that have held up to 1.8 million individuals from predominantly Muslim ethnic minority groups, including Uyghurs, Kazakhs, Kyrgyz, Hui, and others." *Ibid.*

This ongoing "harassment and intimidation" in the United States has "had a chilling effect on Uyghurs in the United States who wish to speak about repression in [China] and violates their right to freedom of expression and association." *Ibid.* That chill is intensified when, as often happens, China attacks Uyghurs by threatening their family members.

"The Chinese government often harasses Uyghurs in the United States by forcing [them] to convey sensitive personal and financial information" to "close family members" in China. *Ibid.* "In one mid-2018 case," for example, "a Uyghur woman living in the United States was contacted by her mother and asked to provide—in addition to her U.S. phone number—her U.S. bank account number and the license plate number of her car." *Ibid.* "In another similar 2018 incident, Chinese authorities detained the mother of Uyghur-American Ferkat Jawdat in a [Chinese] mass internment camp, prompting Jawdat to speak out about her plight. He would not hear from his mother again until more than a year later, in a May 2019 phone call, when she said she had been released from the camp[] and asked him to cease his advocacy." *Ibid.*

3. In a letter to the Biden Administration, 24 human rights organizations—including Human Rights Watch and ChinaAid—summarized the situation well:

> The scope and scale of human rights violations committed by the Chinese government inside *and outside the country* require a fundamental shift; many of the tools previously employed are no longer relevant or sufficiently robust. We welcome senior officials' statements that the US government will hold the Chinese government "accountable for its abuses of the international system," and the suggestion that the US will impose consequences for serious violations.

A Human Rights Approach to U.S.-China Policy: A Joint NGO Letter to the Biden Administration (Feb. 17, 2021) (emphasis added).

B. China has acted to harass and intimidate ChinaAid and its supporters, even using proxies to make public death threats against ChinaAid's president.

China's transnational repression is anything but hypothetical to ChinaAid. Thanks to its long record of calling attention to China's persecution of Christians, ChinaAid has been labeled by the Chinese Communist Party—via one of its newspapers—as "anti-China." Huang Lanlan & Shan Jie, *U.S. Forces Under Guise of Religion Serve as Anti-China Vanguard of Washington*, Global Times (Oct. 27, 2020). According to the paper, China Aid works with other "anti-China forces"—which it says include certain former members of the U.S. House of Representatives, a leading academic at the University of Texas at Austin, and multiple pro-human rights organizations, including the National Endowment for Democracy and the Lantos Foundation. *Ibid*. All of these supposedly nefarious actors, says the paper, are guilty of forming a "conspiracy of

politicizing religious matters in China" and, in so doing, "break[ing] local order and values." *Ibid.*

But of the forces it labeled "anti-China," China has reserved its strongest ire for the founder of ChinaAid, Bob Fu, who has been publicly threatened with death by a proxy of China who lives in the United States. In September 2020, an exiled businessman from China named Guo Wengui posted a video online urging viewers to "eliminate" Fu and another prominent critic of the Chinese Communist Party, Wu Jianmin, who lives in Southern California: "Let's eliminate traitors in the world. * * * Let's get started, let's finish with these traitors first." Nick Aspinwall, *Guo Wengui is Sending Mobs After Chinese Dissidents*, Foreign Policy (Oct. 28, 2020). When protesters began appearing by the dozens outside Fu's house in Midland, Texas, law enforcement officials advised Fu family members to evacuate and disperse to separate locations, which they did. No. 7:20-cv-00257, *Fu* v. *Wengui*, Doc. 1, at ¶ 16 (W.D. Tex. Nov. 12, 2020) (complaint).

Fu also filed a federal suit against Wengui documenting his multiple public death threats, which now include a price on Fu's head. *Id.* ¶ 16. Posted on Wengui's YouTube and Twitter accounts, as well as on Wengui's own live broadcasting service and personal website, the threats have been explicit and repeated:

- Labeling Fu a "threat to all human beings," in September 2020, Wengui called for his followers to "kill" Fu, as part of a larger, international "Kill Cheaters" campaign.
- The next day, when protesters appeared at Fu's house and he called the police, Wengui posted a new video: "We will send at least 100 to 200 comrades to your house tomorrow.

> We will see how much power you have in the U.S."

- The same day, Wengui posted another video naming Fu on his "Kill Cheaters" campaign hit list, which also included the California pro-democracy activist Wu Jianmin.

- Still on that same day, Wengui intensified his demand: "If you didn't participate in the global kill cheaters [sic] campaign, there's something wrong with you. You need to take actions [sic]. None of those cheaters should be missed. We need to see the result."

Id. ¶¶ 42, 45.

Responding to these demands, one of Wengui's followers went to Jianmin's house in California and filmed himself shouting at Jianmin from the driveway:

> Scumbag Jianmin! And that Bob Fu! Bob Fu * * * [w]ait for me to kill Jianmin Wu first and you'll be the next * * * * You dirtbags milk the First Amendment in U.S. for your freedom of speech * * * * I am not afraid of death * * * * I will go [sic] your houses one after another. Get your guns ready and have your bullets loaded. You'd better shoot me or you just wait and see.

Id. ¶ 46. Wengui posted this video online. *Ibid.*

Wengui then raised the stakes by offering a reward for "comrades" who would "find Bob Fu and kill him":

> I'm appealing again to all the comrades * * * Connect and converge to Midland[,] Texas to find Bob Fu and kill him. This is the time to test

> your loyalty and ability. I will reward you with stocks according to your action. * * * Whether you are a true comrade or not, we will figure it out from your action.

Id. ¶ 47. The next day, Wengui republished his hit list and declared: "They deserve to die"; "the revolution exposed all these bastards." *Id.* ¶ 49. Wengui's online attacks continued through October 2020 and were viewed by hundreds of thousands of people, prompting protesters to threaten Fu online with death and, in one case, to appear at Fu's house to threaten him in person. *Id.* ¶¶ 50-79.

The threats forced Fu to close ChinaAid's offices. Mindy Belz, *Weapons of Mass Distraction*, WORLD Magazine (Oct. 22, 2020). They have also traumatized his family. As he explained to one reporter, "[t]he children are realizing there is a price to pay for religious advocacy, even on U.S. soil." *Ibid.*

What is going on here? In his threatening videos, Wengui does not announce himself as an agent of China; to the contrary, he proclaims himself an anti-communist. *Fu* v. *Wengui*, Doc. 1, at ¶ 20. But in 2017, after he came to the United States, Wengui "appeared in a television interview on Mirror TV, a Chinese language news organization based in New York. In the interview, [he] pledged 'to serve under President Xi' and 'to contribute to President Xi's China dream.'" *Ibid.* And it is common for China to work through proxies. In fact, China maintains "a network of proxy entities" and "activists" who "have been involved in harassment and even physical attacks against party critics and religious or ethnic minority members. The greater distance from official Chinese government agencies offers the regime plausible deniability on the

one hand, while accomplishing the goal of sowing fear and encouraging self-censorship far from China's shores, on the other." Transnational Repression Report 17. That is exactly what happened to Bob Fu.

If Wengui were *not* a proxy of China, moreover, one wonders why he included China critic Wu Jianmin on his hit list. Like Fu, Jianmin "had no prior connections to [Wengui] before the billionaire and his followers began their pressure campaigns, but he believes Chinese authorities are 'very aggravated' by his popular anti-CCP [*i.e.*, Chinese Communist Party] YouTube channel. 'Only the CCP and its agents would desire [the] silencing of my voice,' he said." Aspinwall, *supra.*

C. One of China's primary means of attacking critics outside of China is highly sophisticated hacking, including into federal agencies.

Though China is bold enough to threaten dissidents in the United States directly, it is also savvy enough to rely on skilled hackers to breach U.S. computer systems. The U.S. Director of National Intelligence has ranked the number one worldwide threat to the United States as cyberattacks from China. Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community* 5 (2019). These attacks extend far beyond traditional national security interests; they range into sensitive U.S. human rights and humanitarian information housed in nonprofit and government systems alike.

Most recently, "a group of hackers associated with China's main intelligence service * * * infiltrated more than 100 companies and organizations around the world to steal intelligence, hijack their networks and extort their victims." Katie Benner & Nicole Perlroth,

China-Backed Hackers Broke Into 100 Firms and Agencies, U.S. Says, N.Y. Times (Sept. 16, 2020). The hackers not only "targeted social media and other technology companies," but "universities, government agencies and nonprofits." *Ibid.* According to the U.S. Department of Justice, "the scope and sophistication of the crimes in these unsealed indictments is unprecedented." U.S. Dep't of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally* (Sept. 16, 2020). Particularly alarming was China's use of mercenary hackers, who "believed their association with the PRC provided them free license to hack and steal across the globe." *Ibid.* Other Chinese "state-sponsored hackers broke into the networks of the Vatican to conduct espionage in the lead-up to negotiations about control over the appointment of bishops and the status of churches in China." Center for Strategic & International Studies, *Significant Cyber Incidents 2020-21*; Francis Rocca & Eva Xiao, *China Hacked Vatican Ahead of Negotiations, U.S. Cybersecurity Firm Says*, The Wall Street Journal (July 29, 2020).

Of course, many Chinese hackers also work directly for the Chinese government—such as those who explored "security vulnerabilities in the networks of biotech firms in Maryland, Massachusetts[,] and California that were studying coronavirus vaccines and treatments," along with "a California firm producing coronavirus testing kits." Eric Geller & Betsy Woodruff Swan, *DOJ Says Chinese Hackers Targeted Coronavirus Research*, Politico (July 21, 2020). The coronavirus piece of the operation formed only a small part of the attack. For years, the hackers invaded the systems of "hundreds of victim companies, governments, non-

governmental organizations, and individual dissidents, clergy, and democratic and human rights activists in the United States and abroad." U.S. Dep't of Justice, *Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research* (July 21, 2020). Ominously for ChinaAid—given that Bob Fu helped to organize the Tiananmen Square protests—the hackers "provided their Chinese government contact with the passwords of human rights activists, including a community organizer in Hong Kong and a former Tiananmen Square protester." Geller & Swan, *supra.*

China's hackers have also enjoyed great success penetrating U.S. government agencies. For example, in a highly publicized incursion lasting over a year, "Chinese intruders" gained "administrator privileges" in "the computer networks at the Office of Personnel Management [OPM], mimicking the credentials of people who run the agency's systems." David E. Sanger, Nicole Perlroth, & Michael D. Shear, *Attack Gave Chinese Hackers Privileged Access to U.S. Systems*, N.Y. Times (June 20, 2015). With those credentials in hand, "[t]he hackers began siphoning out a rush of data"—including 5.6 million sets of fingerprints—"after constructing what amounted to an electronic pipeline that led back to China[.]" *Ibid.*; Kaveh Waddell, *5.6 Million Fingerprints Stolen in OPM Breach*, The Atlantic (Sept. 23, 2015).

The successful attack at OPM should have been no surprise. Just the year before, auditors had "harshly criticized lax security at the Internal Revenue Service, the Nuclear Regulatory Commission, the Energy Department, the Securities and Exchange Commission—

and the Department of Homeland Security, which has responsibility for securing the nation's critical networks." Sanger, Perlroth, & Shear, *supra*. "At the Nuclear Regulatory Commission * * * information about crucial components was left on unsecured network drives, and the agency lost track of laptops with critical data." *Ibid*. "Computers at the I.R.S. allowed employees to use weak passwords like 'password'"; and "[o]ne report [on the IRS] detailed 7,329 'potential vulnerabilities' because software patches had not been installed." *Ibid*. The same year that OPM was hacked, the IRS was too. "[I]dentity thieves used one of its online services to obtain prior-year tax return information for about 100,000 U.S. households." John D. McKinnon & Laura Saunders, *Breach at IRS Exposes Tax Returns*, The Wall Street Journal (May 26, 2015).

D. China's hackers are among the world's most elite; they have hacked the "Holy Grail of cyberespionage": the iPhone.

Like all hackers, China's hackers "exploit[] publicly disclosed vulnerabilities in widely used software[.]" Geller & Swan, *supra*. Indeed, the two Chinese hackers discussed above, who were indicted for breaking into hundreds of companies and nongovernmental organizations, "took advantage of newly announced vulnerabilities before companies had had time to patch them." *Ibid*. But China does not *need* known vulnerabilities. For example, China's government allegedly gave one of the hackers a "zero-day exploit," which is "a highly valuable piece of code designed to compromise a previously unknown flaw." *Ibid*.

So capable has China become at finding flaws, in fact, that Google has discovered—and Apple has admitted—that China has hacked into the iPhone.

Nicole Perlroth, Kate Conger, & Paul Mozur, *China Sharpens Hacking to Hound Its Minorities, Far and Wide*, N.Y. Times (Oct. 22, 2019). At least for a time, even the FBI could not do this. In 2016, the FBI obtained multiple court orders requiring Apple to help the FBI break into an iPhone to investigate "a gunman involved in the killing of 14 people" in California. *Ibid.* When Apple refused to comply, the FBI "paid more than $1 million to an anonymous third party to hack" into the iPhone. *Ibid.*

But more recently, "Google researchers said they had discovered that iPhone vulnerabilities were being exploited to infect visitors to a set of websites. Although Google did not release the names of the targets, Apple said they had been found on about a dozen websites focused on [Uyghurs]." Perlroth, Conger, & Mozur, *supra.*

Once an iPhone is breached, its user can be monitored. That is why "[b]reaking into iPhones has long been considered the Holy Grail of cyberespionage. 'If you can get inside an iPhone, you have yourself a spy phone,'" according to John Hultquist, director of intelligence analysis at a cybersecurity firm. *Ibid.* Alas, Google's Android phones fared no better; Chinese hackers compromised those phones, too. *Ibid.*

II. China's sophisticated hackers will inevitably exploit California's porous registry to find donors to organizations that China views as critics.

California's primitive donor-disclosure registry is no match for the skill and ferocity of China's hackers. As the Ninth Circuit conceded, the registry revealed its entire contents—350,000 documents—to the public, and affirmatively mislabeled as public some 1,800

donor lists. AFPF Pet. 36a; TMLC Pet. 39-40a. The court drew comfort from the State's promises that its security problems were solved. TMLC Pet. 40-41a; AFPF Pet. 36-37a. But at every turn, the court's analysis unwittingly highlights the ongoing flaws in the registry, which China will inevitably exploit.

A. The decision below inadvertently highlights the ruinous defects in California's registry.

1. California *still* uploads the entire contents of its registry—60,000 donor lists—to the Internet every year.

According to the Ninth Circuit, "much of" California's error in labeling some 1,800 lists public "can be traced to the large amount of paper the Registry Unit processes around the same time each year. The Registry Unit receives over 60,000 registration renewals annually, and 90 percent are filed in hard copy." AFPF Pet. 36a; TMLC Pet. 40a. One might view this as a red flag suggesting that the State is running needless risks by uploading voluminous renewals onto the Internet in the first place. After all, almost two decades before the Internet existed, this Court warned of "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." *Whalen* v. *Roe*, 429 U.S. 589, 605 (1977). Ignoring this well-established risk, the State insists on "uploading" the donor lists. AFPF Pet. 36a; TMLC Pet. 40a.

2. The "tedious" task of uploading 60,000 donor lists is *still* left to "temporary" and "student" workers, whose errors the State does not count as public disclosures.

Compounding the risk of disclosure, the State continues to entrust the sensitive task of uploading donor lists to "temporary workers and student workers." AFPF Pet. 36a; TMLC Pet. 40a. Unsurprisingly, given the "volume and tediousness of the work," the students and temporary workers "occasionally mismark[] [the lists] as public and then upload[] them to the public-facing site." *Ibid.* But here again, rather than declining to upload the lists, or hiring skilled workers, the State has decided only to "implement[] stronger protocols," including "procedural quality checks[.]" AFPF Pet. 36a-37a; TMLC Pet. 40a.

One must question California's will to enforce its new protocols however, given that it does not view inadvertent disclosures as breaches. Indeed, according to the head of the State's donor registry, "if every confidential [donor list] ever obtained by the registry were inadvertently uploaded for public access via links and publicly downloaded, there would [be] no breach of the confidentiality policy[.]" AFPF JA 423. Similarly, the former registry head testified that she did not consider confidential material appearing online to be "public disclosures" at all if, "as far as we know, *nobody had viewed* the documents." ER 768 (emphasis added).[2] Not surprisingly, then, the State does not penalize

[2] "ER" refers to the excerpts of record filed with the Ninth Circuit in Nos. 16-55727 & 16-55786 at Dkt. 9.

inadvertent disclosures; indeed, it does not even penalize intentional disclosures. TMLC JA 285-86.

In short, the State has adopted stronger protocols to avoid what it maintains are non-breaches triggering no consequences. That does not inspire confidence.

3. Donor lists are *still* "inadvertently misclassified as public" and left public on the Internet for up to six days.

Even the Ninth Circuit conceded that the new protocols will falter and documents still be "misclassified as public." AFPF Pet. 37a; TMLC Pet. 41a. But once again, instead of abandoning its effort to upload 60,000 lists to the Internet, the State has chosen to implement another "system"—this one automated—that involves running a "weekly script to identify and remove any documents that it had inadvertently misclassified." AFPF Pet. 37a; TMLC Pet. 40a-41a. Left unstated, of course, is that removing confidential documents "weekly" leaves them online for up to six days. That is plenty of time for even sluggish hackers to find them.

4. The State *still* relies on charities themselves to catch its errors and demand they be fixed "immediately."

California will remove publicized donor lists "immediately" only if someone discovers the problem before hackers do and flags it for the State. AFPF Pet. 37a; TMLC Pet. 41a. In other words, California demands that the final protection for the 60,000 donor lists that it *insists* that charities submit, and that it *insists* on uploading to the Internet using students and temporary workers, and that it *insists* on double-checking only weekly, is the 60,000 charities themselves. In a footrace between China's hackers and the

staff of American charities, who have been assured their lists are secure, there is little doubt who will win.

5. It is no answer to say, as does the decision below, that "nothing is perfectly secure on the [I]nternet," especially as the State stores *hard copies* of donor lists with unmonitored outside vendors.

Not to worry, says the Ninth Circuit: "Nothing is perfectly secure on the [I]nternet in 2018, and the Attorney General's data are no exception, but this factor alone does not establish a significant risk of public disclosure. * * * [A]ny regulation * * * comes with some risk of abuse." AFPF Pet. 37a; TMLC Pet. 41a.

This statement is mistaken three times over. One, it assumes that donor lists must be placed on the Internet at all. Two, it assumes the donor lists are "the Attorney General's data." Three, it assumes that the "significant risk of exposure" is caused by placing the donor lists on the Internet "alone." None of these assumptions is valid. The donor lists do *not* need to be placed on the Internet (indeed, they largely do not need to be collected at all; *see* AFPF Br. 31-39; TMLC Br. 35-38, 40-43). The lists are the data of the *charities* that disclosed them. And the lists' risk of public exposure, though dramatically heightened by needlessly placing them on the Internet, is raised further still by the State's decision to use unskilled workers to upload the lists and check for mistakes only once a week.

The risk of exposure is heightened yet again by California's decision to store *hard copies* of donor lists with an unmonitored outside vendor called "Pacific Storage." AFPF JA 372. The State has never confirmed with Pacific Storage that it follows any of the State's confidentiality policies; nor does the State

know "anything" about Pacific Storage's "methods and procedures" to "maintain confidentiality." *Id.* at 376-77. The State also has "no idea" of "how many people at Pacific Storage may have access to [donor lists]." *Id.* at 377. In fact, the State does not know "anything about the extent to which members of the public can go to Pacific Storage and access archives." *Ibid.*

Hard copies aside, California's electronic registry is an "open door for hackers." AFPF Pet. 92a; TMLC Pet. 123a. And that is not the result of parties supposedly complaining about "any regulation at all." AFPF Pet. 37a; TMLC Pet. 41a. It is the result of deliberate choices made by the State of California.

B. California will not be able to stop China if it could not stop petitioner's expert *after* he notified the State of a major flaw in the registry.

Finally, a natural experiment has already been run on California's ability to secure its donor registry against a known attack, at a known time, against a known weakness. The registry failed.

Before trial, petitioner's expert "probed the Registry's servers for flaws" and found "approximately 1800 confidential [donor lists] that had been misclassified as public over several years." AFPF Pet. 35a-36a; TMLC Pet. 39a-40a. According to the Ninth Circuit, "the Attorney General promptly removed them from public access." AFPF Pet. 36a; TMLC Pet. 40a. But even after this massive error was exposed, the State failed to secure the donor lists. As the district court found, "the day before * * * trial," the expert found "38 more" confidential donor lists on the public website. AFPF Pet. 52a.

In light of this, one must ask: If California cannot secure donor lists when it knows exactly *how* those lists were compromised, by *whom* they were compromised, and *when* that same person will likely try to access them again, what assurance can anyone have that the State will have any luck protecting lists from China's experts who can hack the iPhone?

III. Given the speed and ferocity of China's extraterritorial repression, an as-applied challenge would be useless to groups like ChinaAid.

As petitioners have shown, California's mandate should be struck down facially because it is anything but narrowly tailored. AFPF Br. 30-45; TMLC 33-38. After all, "[w]e are in an area where * * * any regulation must be highly selective in order to survive challenge under the First Amendment." *La. ex rel. Gremillion* v. *NAACP*, 366 U.S. 293, 295-97 (1961). And the mandate is the opposite of "highly selective." *Ibid.* But the mandate should be struck down facially for another reason. It cannot *be* attacked meaningfully in as-applied challenges by groups like ChinaAid, who will not know that their donor lists have been stolen before it is too late. At that point, the cat will be out of the bag. The thieving nation-state will have the names and addresses it needs to launch its campaign of repression against donors across the United States.

The only solution to this problem is to prevent it. And the only way to prevent it here, particularly given California's implacable determination to post 60,000 donor lists on the Internet every year, is to strike down the mandate wholesale.

Just as "[t]he First Amendment does not permit laws that force speakers to retain a campaign finance

attorney * * * or seek declaratory rulings before discussing the most salient political issues of our day" (*Citizens United* v. *FEC*, 558 U.S. 310, 324 (2010)), it does not require human rights organizations to retain counsel to seek injunctions protecting information that has already been stolen. That would only "prolong the substantial, nationwide chilling effect" (*id.* at 333) created by California's blanket mandate, but to no use. And that would make no sense. This Court has been willing to forgo "case-by-case determinations" if "archetypical" First Amendment rights "would be chilled in the meantime." *Id.* at 329. That is the case here.

Indeed, the Court should be all the more willing to forgo case-by-case rulings here, where the "chill" comes from powerful nation-states with track records of using the Internet to steal with impunity and make good on their threats. Given the adversaries in question, the Court should not "endorse a view of the First Amendment that subjects citizens of this Nation to death threats * * * as the price" for engaging in the "freedom of association" protected by the First Amendment. *Id.* at 485 (Thomas, J., dissenting); *NAACP* v. *Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958).

* * *

In the age of the Internet, the speed of extraterritorial repression is the speed of light. As a result, groups like ChinaAid, and courageous dissidents like Bob Fu, cannot afford to wait to bring an as-applied challenge to the inevitable theft of their donor lists by China. By then it will be too late. The Court should strike down California's mandate in its entirety.

CONCLUSION

For the foregoing reasons, the judgment below should be reversed.

Respectfully submitted,

SEAN P. GATES
Charis Lex P.C.
301 N. Lake Ave.
Ste. 1100
Pasadena, CA 91101
(626) 508-1715
sgates@charislex.com

ANDREW C. NICHOLS
Counsel of Record
Charis Lex P.C.
4250 N. Fairfax Dr.
Ste. 600
Arlington, VA 22203
(571) 549-2645
anichols@charislex.com

Counsel for Amicus Curiae

MARCH 2021