No. G058506

COURT OF APPEAL, STATE OF CALIFORNIA
FOURTH APPELLATE DISTRICT
DIVISION THREE

FRIENDS FOR FULLERTON'S FUTURE, JOSHUA FERGUSON, and DAVID CURLEE
Petitioners,

v.

SUPERIOR COURT OF THE STATE OF CALIFORNIA, COUNTY OF ORANGE
Respondent,

CITY OF FULLERTON,
Real Party in Interest.

APPEAL FROM THE SUPERIOR COURT FOR
THE COUNTY OF ORANGE
Hon. Thomas A. Delaney, (657) 622-5224
Superior Court No. 30-2019-01107063-CU-NP-CJC

APPLICATION FOR LEAVE TO FILE AMICUS CURIAE BRIEF AND PROPOSED AMICUS BRIEF OF THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS IN SUPPORT OF PETITIONERS

*Katie Townsend (SBN 254321)
**Counsel of Record*
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1020
Washington, D.C. 20005
Telephone: (202) 795-9300
Facsimile: (202) 795-9310
ktownsend@rcfp.org

APPLICATION FOR LEAVE TO FILE AMICUS CURIAE BRIEF

TO THE HONORABLE PRESIDING JUSTICE AND ASSOCIATE JUSTICES OF THE FOURTH APPELLATE DISTRICT, DIVISION THREE:

Pursuant to California Rule of Court 8.200(c), the Reporters Committee for Freedom of the Press respectfully requests leave to file the attached brief as amicus curiae in support of Petitioners Friends for Fullerton's Future, Joshua Ferguson, and David Curlee.

Founded in 1970 by journalists and media lawyers following an unprecedented wave of government subpoenas forcing reporters to name confidential sources, the Reporters Committee serves as a leading voice for the legal interests of working journalists and news organizations. The Reporters Committee's Technology and Press Freedom Project works extensively on legal and policy issues at the intersection of federal computer crime law and press rights. *See* Gabe Rottman & Lyndsey Wajert, *Scraping Public Websites Likely Doesn't Violate the Computer Fraud and Abuse Act*, Reporters Comm. for Freedom of the Press (Sept. 19, 2019), https://perma.cc/XBQ3-GF7D.

As an organization dedicated to defending the First Amendment and newsgathering rights of journalists, the Reporters Committee submits the proposed amicus brief to aid the Court by underscoring the profound threat posed to journalism, especially data journalism, by the City of Fullerton's

legal theory in this lawsuit.

This Application is made on grounds that the proposed amicus brief would assist the Court in ruling on—and denying—the relief sought by the City of Fullerton. Proposed Amicus represents the interests of local, state, and national news organizations and journalists throughout California and the nation. The Reporters Committee has substantial knowledge and expertise concerning federal and state laws pertaining to the use of technology, and how interpretations of those laws may impact journalists.

The proposed amicus curiae brief outlines how Plaintiff's claims against the Defendants pose a severe threat to newsgathering. Plaintiff asserts that Defendants have violated the Computer Fraud and Abuse Act and the California Comprehensive Computer Data Access and Fraud Act, which are intended to address "hacking." The conduct alleged here, however, does not amount to "hacking." Indeed, the records Plaintiff alleges Defendants accessed were not obscured by a password or any other technical barrier that was meant to keep these allegedly sensitive and privileged materials hidden. Defendants are essentially accused of accessing records that were made publicly available by Plaintiff via a Dropbox account.

Further, Plaintiff misleadingly attempts to argue that Defendants' alleged use of encrypted security services such as virtual private networks ("VPNs") or anonymizing browsers such as The Onion Router ("Tor")

reflects a sinister and malicious intent. Yet, as explained in the proposed amicus brief, the use of these types of services is both commonplace among journalists and recommended by the Reporters Committee, among others, as a best practice in the industry.

For these reasons, the Reporters Committee respectfully requests that the Court grant this Application and accept the proposed amicus curiae brief below.

Dated: November 5, 2019

Respectfully submitted,

REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
Katie Townsend (SBN 254321)

Katie Townsend
Counsel of Record for Amicus Curiae

No. G058506

COURT OF APPEAL, STATE OF CALIFORNIA
FOURTH APPELLATE DISTRICT
DIVISION THREE

FRIENDS FOR FULLERTON'S FUTURE, JOSHUA FERGUSON, and DAVID CURLEE,
Petitioners,

-vs-

SUPERIOR COURT FOR THE STATE OF CALIFORNIA, COUNTY OF ORANGE
Respondent,

CITY OF FULLERTON,
Real Party in Interest.

APPEAL FROM THE SUPERIOR COURT FOR
THE COUNTY OF ORANGE
Hon. Thomas A. Delaney, (657) 622–5224
Superior Court No. 30-2019-01107063-CU-NP-CJC

AMICUS BRIEF OF THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS IN SUPPORT OF PETITIONERS

*Katie Townsend (SBN 254321)
**Counsel of Record*
Bruce D. Brown**
Gabriel Rottman**
Linda Moon**
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1020
Washington, D.C. 20005
Telephone: (202) 795-9300
Facsimile: (202) 795-9310
ktownsend@rcfp.org
** *Of counsel*

CERTIFICATE OF INTERESTED ENTITIES OR PERSONS

Pursuant to California Rule of Court 8.208(e)(1) and (2), the Reporters Committee for Freedom of the Press, by and through its undersigned counsel, certifies that it is an unincorporated nonprofit association of reporters and editors with no parent corporation or stock. The Reporters Committee has no financial or other interest in the outcome of this proceeding that the justices should consider in determining whether to disqualify themselves.

Dated: November 5, 2019

Katie Townsend
Counsel of Record for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

The Reporters Committee for Freedom of the Press (the "Reporters Committee") respectfully submits this amicus curiae brief to highlight the profound threat to journalism—especially data journalism—posed by the legal theory deployed by the City of Fullerton (the "City") in this lawsuit.

The essence of the City's allegations in this case is that bloggers reporting on newsworthy matters of clear public interest (namely, potential government misconduct) violated federal and state hacking laws by accessing information that was made available online by the City to all the world. The City claims it is entitled not only to an extraordinary prior restraint on publication but also damages, in part for claims against the City for breach of confidentiality caused by the City's own cybersecurity lapses.

Amicus is not aware of any case where federal or state hacking laws have been misused so brazenly to target routine newsgathering activities—namely, the collection of government information available to any internet user. Journalists, and data journalists in particular, who often use computer programs to collect large amounts of data online (known as "scraping" or "spidering"), however, have long expressed concern that such laws could be misused to penalize the collection of publicly available information on the internet—a concern shared by Amicus and other news media organizations and press freedom advocates.

As an initial matter, the Reporters Committee agrees with Petitioners that the temporary restraining order entered below is a prior restraint on the publication of information in the public interest that should be immediately vacated. Prior restraints are "the most serious and the least tolerable infringement on First Amendment rights" because they are "an immediate and irreversible sanction," not only "chilling" speech but also "freezing" it, at least for a time. *Nebraska Press Ass'n v. Stuart* (1976) 427 U.S. 539, 559. Indeed, even where the government claimed that publication would result in serious national security harm, the U.S. Supreme Court has held that a bar for a prior restraint was not met. *See N.Y. Times Co. v. United States* (1971) 403 U.S. 713 (rejecting injunctive relief against publication of stories based on secret history of Vietnam War, known as the Pentagon Papers); *see also Near v. Minnesota* (1931) 283 U.S. 697.

In addition, the "hacking" theory advanced by the City here also poses an acute threat to press rights. Amicus writes to aid the Court by briefly explaining why that is the case and providing background concerning the appropriate scope of both the federal Computer Fraud and Abuse Act ("CFAA"), passed as part of the Comprehensive Crime Control Act of 1984 (Pub. L. No. 98-473 (Oct. 12, 1984) 98 Stat. 1976) and codified at 18 U.S.C. § 1030, and the California Comprehensive Computer Data Access and Fraud Act, Pen. Code § 502.

Amicus also seeks to emphasize that the use of anonymizing encryption software is not nefarious, as suggested by the City. It is a crucial best practice for information security, particularly for journalists.

ARGUMENT

I. The alleged conduct does not amount to hacking.

First, a review of the technical facts is warranted. If Amicus's reading of the declaration of the City's information technology expert is correct, one did not even need a username or password to access files in the Dropbox account maintained by the City, in which it commingled allegedly sensitive and privileged information with material that it affirmatively invited public records requesters to download.[1] Decl. of Matthew Strebe ¶¶ 16-19, City of Fullerton v. Friends for Fullerton's Future, et al., Case No. 30-2019-01107063 (S. Ct. Cal. Oct. 24, 2019). Conceding that point, Strebe states: "An unlocked door is not a defense to burglary." *Id.* ¶ 19.

[1] The passwords shared by the City were to "unzip" several files. When data files are too large to send via email, they can be compressed or "zipped" to permit sending. Michael Gonyar, *How to Share Large Files Over the Internet*, How-To Geek (May 8, 2018, 6:40 AM), https://perma.cc/U3XE-NVC8. In the exhibits to Klein's declaration, the City provided the password to Petitioners for each of the zipped files, but it does not appear that the City's Dropbox account was itself password protected. *See* Decl. of Mea Klein, Exs. A and E, City of Fullerton v. Friends for Fullerton's Future, et al., Case No. 30-2019-01107063 (S. Ct. Cal. Oct. 24, 2019).

Analogies between the digital and physical world are often inapposite, but to the extent they are helpful, there was no door, let alone a lock in this case. The better analogy is an open, unfenced field that one has actually been invited onto.

To analogize directly to trespass law, the City is effectively arguing that an invitee to one part of a field "should have known" that moving to another part would transform them into a trespasser. Mem. of Points and Authorities in Support of Pl.'s Ex Parte Appl. for a TRO and Order to Show Cause Why a Prelim. Inj. Should Not be Issued at 3, City of Fullerton v. Friends for Fullerton's Future, et al., Case No. 30-2019-01107063 (S. Ct. Cal. Oct. 24, 2019). But without actual notice that a portion of the field is off limits, an invitee cannot transform into a trespasser. *See Powell v. Jones* (1955) 133 Cal.App.2d 601, 606-07 (explaining that an individual could lose his or her invitee status by leaving the "part of the premises neither expressly nor impliedly covered by the invitation"). In the world of computer crime, even actual notice may not be enough to transform access into a prohibited "hacking."

The City appears to have been relying solely on what information security experts call "security by obscurity" to protect the pre-review documents that it commingled with ready-to-release batches of public records in a single Dropbox account. With respect to the public internet, security by obscurity techniques are often applied to internet addresses that,

while accessible by anyone with internet access, would be hard to guess (normally, such addresses contain long strings of randomized numbers, letters, and symbols).

Here, the City sent links to specific folders in its commingled Dropbox account and seemed to expect that either a user would not know she could access other folders in the account, or "should have known" that such folders contained information that was not ready for public release. This expectation appears to be the sole security feature the City implemented.

Moreover, according to the City's own exhibits, the City would also occasionally send public records requesters, including one of the Petitioners, the top-level address for the Dropbox account, which would then present that member of the public with links to all of the sub-folders, including both the pre-review and ready-to-release documents. *See* Decl. of Mea Klein ¶ 11, City of Fullerton v. Friends for Fullerton's Future, et al., Case No. 30-2019-01107063 (S. Ct. Cal. Oct. 24, 2019). The City would then simply provide the name of the relevant subfolder in its email to the public records requester.

While properly implemented security by obscurity techniques can be helpful in information security practices, sole reliance on such a technique is disfavored. As applied to the City's Dropbox account, as soon as someone knows that the City commingles pre-review and ready-to-release

documents in a single unsecured Dropbox account, the use of individualized links is no longer an effective security measure.

Amicus takes no position on the City's information security practices. But the fact that the City commingled pre-review and ready-to-release public records in a publicly accessible Dropbox account without requiring even a password for access is legally relevant in two interrelated ways.

First, the City claims that the "actions of [Petitioners] have placed [it] in a position to defend against claims of breach of confidentiality and have potentially put at risk the security of protected information of both employees and members of the public." *See* Press Release, City Files Superior Court Complaint Against Local Blog, City of Fullerton (Oct. 24, 2019), https://perma.cc/VV3F-MJZR. Such a claim presents an important causation question that is relevant not just to this case but also any other case involving an inadvertent disclosure that could subject a government entity to potential liability for breach of confidentiality.

In this case, if the City failed to properly secure the pre-review information, making it available to the entire world in a publicly accessible Dropbox account, that would be the proximate cause of any breach of any duty of confidentiality owed by the City. Were a government entity able to sue the press for publishing information it made available as a result of poor information security practices merely because the entity could be

subjected to a breach of confidentiality claim, the potential chill on newsgathering would be significant. *Cf. Florida Star v. B.J.F.* (1989) 491 U.S. 524, 538 ("That appellant gained access to the information in question through a government news release makes it especially likely that, if liability were to be imposed, self-censorship would result.").

Second, as discussed at greater length in sections II and III below, this is not hacking. Data journalists and researchers routinely "scrape"—that is, use computer programs to automatically collect information from the public internet en masse. This data is then used to produce important reporting on issues as diverse as invidious discrimination, the courts, and local government. Noa Yachot, *Your Favorite Website Might Be Discriminating Against You*, ACLU (June 29, 2016, 9:45 AM), https://perma.cc/6W67-68J4; Amanda Aronczyk, *Philadelphia Collects Court Debt Decades Later*, Marketplace (Dec. 20, 2012), https://perma.cc/2SAB-7N28; Fedor Zarkhin & Lynne Terry, *Kept in the Dark: Oregon Hides Thousands of Cases of Shoddy Senior Care*, Oregonian/Oregonian Live (Apr. 22, 2019), https://perma.cc/BKL4-6GRD; Ryan Thornburg, *N.C. Data Dashboard Helps Newsrooms Scrape Public Data*, MediaShift (Sept. 24, 2015), https://perma.cc/7RKU-GYPL. Indeed, such newsgathering techniques are becoming all the more important to the free flow of information to the electorate, as the amount of and detail in

online data continue to grow through technological advancements.[2] To the extent federal or state computer crime laws could be used against journalists in civil lawsuits or criminal actions based on that conduct, such laws pose a significant threat to First Amendment-protected activity.

A public website, including the Dropbox account here, is not like a "house." When an entity chooses to make information available to the public on the internet, without a technical access restriction like a password, that information can legally be accessed by anyone. Were that not the case, websites could trigger criminal or civil liability by fiat, through changes in the terms of use of the website, which is exactly what the City is attempting to do here (the City only communicated its desire that the pre-review material not be downloaded in early July, and it does not

[2] In 1988, the Atlanta Journal-Constitution published "The Color of Money," a landmark data journalism series that analyzed mortgage lending data from the government and financial institutions showing that African-Americans in Atlanta were offered and approved for housing loans at vastly lower rates than similarly situated whites (even lower than poorer whites). *See* Investigative Classics: 'The Color of Money,' on Housing Redlining, 1988, RealClearInvestigations (Apr. 10, 2018), https://perma.cc/CSD7-QMFJ. The reporting led to passage of the 1988 amendments to the Fair Housing Act that gave the Department of Housing and Urban Development the authority to investigate and punish housing discrimination. Were the series to run today, the outlet would likely have relied on scraping to build its lending datasets. It also likely would have considered using test accounts on Facebook or other websites to see if African Americans were being advertised housing credit products on the same terms as whites. Under a broad interpretation of the statute, this type of reporting could potentially violate the CFAA, despite it being both legal and of profound value to the public interest when done offline.

allege that Petitioners accessed the material following that cease-and-desist notification). *See* Mem. in Support of Pet. for Alternative and Peremptory Writs of Mandamus, Prohibition, and Review at 36. As discussed in more detail below, the Ninth Circuit recently rejected such an interpretation of federal law with respect to the scraping of publicly available information. *See hiQ Labs v. LinkedIn* (9th Cir. 2019) 938 F.3d 985.

II. This Court should reject the City's overly broad, incorrect interpretation of the Computer Fraud and Abuse Act.

The CFAA was enacted to address computer hacking (the use of technical means to circumvent a technical access restriction like a password). Congress, however, never defined what it means to access a computer "without authorization" or in a way that "exceeds" authorized access, the main triggers of liability, both criminal and civil, under the law. 18 U.S.C. § 1030(a).

Consequently, both prosecutors and private companies have sought to expand the law beyond what information security experts consider to be "hacking," such as mere violations of a websites' terms of use, which often prohibit things like automated data collection. This case closely resembles that scenario except it does not appear that the City had even set any express terms of use for its Dropbox account prior to the cease-and-desist notification.

An overly broad interpretation of "without authorization" imposes liability on activities that are both routine and innocuous. *See* Gabe Rottman, *Knight Institute's Facebook 'Safe Harbor' Proposal Showcases Need for Comprehensive CFAA Reform*, Reporters. Comm. for Freedom of the Press (Aug. 6, 2018), https://perma.cc/34C3-DJRE. Fortunately, several federal courts have adopted a limiting interpretation of the law to confine it to its original purpose. *See, e.g.*, *United States v. Valle* (2d Cir. 2015) 807 F.3d 508, 527 (applying the rule of lenity in holding that Defendant did not violate the CFAA by using his authorized computer access for personal use); *Dresser-Rand Co. v. Jones* (E.D. Pa. 2013) 957 F.Supp. 2d 610, 613 (dismissing CFAA claims, noting that the purpose of the CFAA was to create a cause of action against "hackers" or "electronic trespassers").

Notably, in September 2019, a three-judge panel of the United States Court of Appeals for the Ninth Circuit embraced this "hacking" approach to the CFAA, affirming a declaratory ruling that collecting publicly available data via "scraping" does not constitute access "without authorization" under the statute. *hiQ*, 938 F.3d at 1003. In doing so, the Ninth Circuit noted that it looked to "whether the conduct at issue is analogous to breaking and entering," and found it was not. *Id*. at 1001 (internal quotation marks omitted).

In short, imposing liability for accessing publicly available material on the internet will reach far beyond hacking to sweep in core newsgathering activities.

III. This Court should reject the City's overly broad, incorrect interpretation of the California Comprehensive Computer Data Access and Fraud Act.

As with the CFAA, California's state analog is correctly interpreted as being restricted in scope. Indeed, many California courts properly adhere to the notion that section 502's purpose is to target technical intrusions—hacking—into computers.

Section 502's plain text confirms this view. The relevant subsection imposes liability on an individual who "knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." Pen. Code § 502(c)(2). Section 502(b)(1) in turn states: "'Access' means to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the *logical, arithmetical, or memory function resources* of a computer, computer system, or computer network" (emphasis added). This language, as a leading appellate case aptly noted, "defines 'access' in

terms redolent of 'hacking' or breaking into a computer." *Chrisman v. City of Los Angeles* (2007) 155 Cal.App.4th 29, 34.[3]

The requirement that there be technical interference has proven dispositive in many cases. In *Chrisman*, the court of appeal rejected the application of section 502 to a police officer, who made personal use of his law enforcement database access to search for information about friends and celebrities, stating that his actions did not entail "hacking the computer's 'logical, arithmetical, or memory function resources.'"[4] 155 Cal.App.4th at 35.

Another court, in dismissing a section 502 claim against a former employee who withheld a company password, noted the important distinction between "vexing" behavior, which does not carry liability, and "hacking," which does. *Welenco, Inc. v. Corbell* (E.D. Cal. 2015) 126

[3] The City argues, as noted in *United States v. Christensen* (9th Cir. 2015) 828 F.3d 763, section 502's use of the phrase "knowing access," rather than "unauthorized access" as in the CFAA means section 502 may encompass all sorts of non-technical access. *See* Mem. of Points and Authorities in Support of Pl.'s Ex Parte Appl. for a TRO and Order to Show Cause Why a Prelim. Inj. Should Not be Issued at 8*, supra.* Aside from the fact that *Christensen* is a federal case that has never been cited, let alone applied, by any California court of appeal, the court there also explicitly acknowledged that section 502 is susceptible of the alternate interpretation in *Chrisman* requiring "knowing access" to include activity resembling hacking. 828 F.3d at 789.

[4] It is important to note that the misuse of government databases by government employees can be a punishable offense, just not as a general computer crime.

F.Supp.3d 1154, 1170. By contrast, section 502 was found to apply to a system administrator who coded a government computer system to lock out users and delete data if others tried to access the system precisely because he utilized his technical expertise to effectuate the harm. *People v. Childs* (2013) 220 Cal.App.4th 1079, 1105.

Importantly, even "improper computer inquiries" by an individual who already has access to a database does not fall within the statute's purview. *Chrisman*, 155 Cal.App.4th at 35. Again, section 502 does not reach the "ordinary, everyday use of a computer," but rather a technical break-in. *Id.* at 34.

Section 502, like the federal CFAA, is and should be about hacking.

IV. The use of virtual private networks, Tor, and other encryption software or applications are accepted best practices for information security, particularly for journalists.

The City alleges that Petitioners "utilized methods to mask their identity and computer locations in order to cover up their unauthorized accesses into and downloads from the City's Dropbox account." Compl. at 4, City of Fullerton v. Friends for Fullerton's Future, Case No. 30-2019-01107063 (S. Ct. Cal. Oct. 24, 2019). Further, the City's expert stated: "[W]hether legitimate or illegitimate, the use of anonymizing VPNs is an intentional act knowingly seeking to cover one's tracks while accessing certain websites or networks." Decl. of Matthew Strebe, ¶ 25, *supra*.

In this context, VPNs—virtual private networks—use encryption to safely move data across a public network (the internet) as if it were on a secure private network like one might have at work. VPNs offer many benefits and are strongly recommended when using unsecured public wi-fi networks like in an airport or coffee shop, where internet traffic could conceivably be intercepted in readable form. Tor refers to software, initially conceived by Navy scientists, that obscures the source of a request for data at every transmission point in order to anonymize its source.

It is true that the use of a VPN and Tor serves to protect user anonymity, and that "even some journalists routinely use" them. *Id*. Indeed, the use of such services is not only commonplace among journalists—it is a recommended industry practice. *See* Br. of Amicus Curiae Elec. Frontier Found. at 1, United States v. Matish, No. 4:16-cr-16 (E.D. Va. May 9, 2016); *see also* Rae Hodge, *How to Become a Privacy Ninja: Use These Journalist Tools*, CNET (July 24, 2019), https://cnet.co/2BVlHdV; Roland Bednarz, *4 Digital Security Tips Every Journalist Needs to Know*, Global Investigative Journalism Network (Oct. 22, 2018), https://perma.cc/FV5Z-WSS3. Amicus routinely recommends that journalists use encrypted applications and services to protect the confidentiality of reporter-source communications.

In recent so-called "leak" cases involving the prosecution of journalistic sources for the unauthorized disclosure of government

information to members of the news media, prosecutors have sought to portray the use of encryption by reporters and sources as somehow indicative of malicious intent. *See* Press Release, Former Intelligence Analyst Charged with Disclosing Classified Information, Dep't of Justice (May 9, 2019) https://perma.cc/EK35-R9CB; Press Release, Former U.S. Senate Employee Indicted on False Statements Charges, Dep't of Justice (June 7, 2018), https://perma.cc/53YZ-PZ4Z. It is not. Everyone should be using encrypted services and applications to protect their communications. In fact, in 2017, the American Bar Association's Committee on Ethics and Legal Responsibility recommended that lawyers use "high level encryption" or other "strong protective measures" to protect sensitive client information. *See* ABA Formal Opinion 477R (Revised May 22, 2017), https://perma.cc/B4GN-7E22; *Did That Email Breach Legal Ethics? Why the ABA Issued Formal Opinion 477 and How to Respond*, Thompson Reuters, https://perma.cc/Q66C-5GKY (last visited Nov. 4, 2019) ("If you communicate with clients electronically—including email, file-exchange services like Dropbox or Google Drive, and text messaging—you need to exercise reasonable effort to make sure this information isn't hacked. If you don't, you're breaching legal ethics."); Kendra Albert, *Computer Security Tools & Concepts for Lawyers*, 20 Green Bag 2d 127 (2017).

While encryption can be used by bad actors to hide bad acts, it is also used by lawyers, domestic abuse victims, the military and law

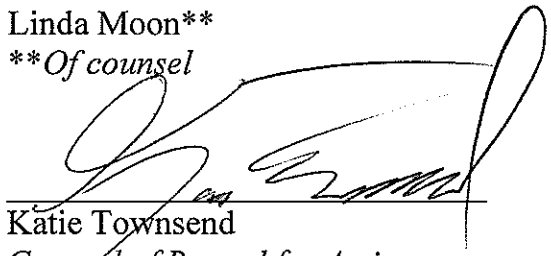
enforcement, political dissidents, and human rights activists, as well as numerous journalists and news organizations.

CONCLUSION

For all of these reasons the Reporters Committee urges this Court to vacate the temporary restraining order.

Respectfully submitted,

REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
Katie Townsend (SBN 254321)
Bruce D. Brown**
Gabriel Rottman**
Linda Moon**
***Of counsel*



Katie Townsend
Counsel of Record for Amicus Curiae

CERTIFICATE OF WORD COUNT

Pursuant to Rule 8.204(c) of the California Rules of Court, I hereby certify that the attached amicus curiae brief was produced using 13-point Roman type, including footnotes, and contains 3,566 words. I have relied on the word-count function of the Microsoft Word word-processing program used to prepare this brief.

Dated: November 5, 2019

Katie Townsend
Counsel of Record for Amicus Curiae

PROOF OF SERVICE

I, Linda Moon, do hereby affirm that I am, and was at the time of service mentioned hereafter, at least 18 years of age and not a party to the above-captioned action. My business address is 1156 15th St. NW, Suite 1020, Washington, D.C. 20005. I am a citizen of the United States and am employed in Washington, District of Columbia.

On November 5, 2019, I served the foregoing documents:

Application for Leave to File Amicus Curiae Brief and Proposed Amicus Curiae Brief of the Reporters Committee for Freedom of the Press in Support of Petitioners as follows:

[x] By email or electronic delivery:

Kelly A. Aviles Law Offices of Kelly Aviles 1502 Foothill Boulevard Suite 103-140 La Verne, CA 91750 kaviles@opengovlaw.com	*Counsel for Defendants and Petitioners Friends for Fullerton's Future, Joshua Ferguson, and David Curlee*
Kimberly Hall Barlow Jones & Mayer 3777 North Harbor Blvd. Fullerton, CA 92835 khb@jones-mayer.com	*Counsel for Plaintiff and Real Party in Interest City of Fullerton*

[x] By mail:

Honorable Thomas A. Delaney
Judge, Dept C24
Orange County Superior Court
700 W Civic Center Dr.
Santa Ana, CA 92701

I declare under penalty of perjury under the laws of the State of California and the United States of America that the above is true and correct.

Executed on November 5, 2019, at Washington, D.C.

By: 

Linda Moon
lmoon@rcfp.org