No. G058996

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

CITY OF FULLERTON
Plaintiff/Respondent,

v.

FRIENDS FOR FULLERTON'S FUTURE, JOSHUA FERGUSON, and DAVID CURLEE
Defendants/Appellants.

APPEAL FROM THE SUPERIOR COURT FOR
THE COUNTY OF ORANGE
The Honorable James L. Crandall, (657) 622-5224
City of Fullerton v. Friends for Fullerton's Future et al.
Superior Court No. 30-2019-01107063-CU-NP-CJC

AMICUS CURIAE BRIEF OF THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS IN SUPPORT OF APPELLANTS

*Katie Townsend
(SBN 254321)
**Counsel of Record*
Bruce D. Brown**
Gabriel Rottman**
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 Rules of Court, rule 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: January 4, 2021

/s/

Katie Townsend
Counsel of Record for Amicus Curiae
Bruce D. Brown**
Gabriel Rottman**
** *Of counsel*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Court Rules

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 allegation in this case is that bloggers reporting on newsworthy matters of clear public interest (namely, potential government misconduct) violated federal and state anti-hacking laws by accessing information that was made available online by the City itself. The City claims it is entitled to an extraordinary prior restraint on publication, in the form of the preliminary injunction granted below.

Amicus is not aware of any case where a federal or state anti-hacking law has been misused so brazenly to target routine newsgathering—namely, the collection of government information available to any internet user.

As an initial matter, the Reporters Committee agrees with Appellants that the injunction entered below is an unconstitutional 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"; they are "an immediate and irreversible sanction" that not only "chills" speech but also "freezes" it. (*Neb. Press Assn. v. Stuart* (1976) 427 U.S. 539, 559 [96 S.Ct. 2791, 49 L.Ed.2d 683].) Indeed, even where the government claimed publication would result in serious harm to national security, the Supreme Court of the United States has held that the bar for a prior restraint had not been cleared. (See *N.Y. Times Co. v. United States* (1971) 403 U.S. 713 [91 S.Ct. 2140, 29 L.Ed.2d 822] [rejecting injunction 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 [51 S.Ct. 625, 75 L.Ed. 1357].)

In addition, the "hacking" theory advanced by the City in this case threatens press rights and, if accepted, would raise serious constitutional concerns with the statutes at issue. Amicus writes to aid the Court by explaining why and to clarify the appropriate scope of both the federal Computer Fraud and Abuse Act ("CFAA"), (see 18 U.S.C. § 1030), and the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), (Cal. Pen. Code, § 502).

ARGUMENT

I. Interpreting either the CFAA or CDAFA to impose liability for routine newsgathering would raise constitutional concerns.

The crux of the City's argument is that accessing cityoffullerton.com/outbox was illegal—even though any computer user could type that URL into her browser and access the linked Dropbox account, without a password—because its existence was not advertised on cityoffullerton.com and because Appellants should have known that the City did not want them to view it. (See Respondent's Br. 17.) As explained in more detail below, the City is wrong. Neither the CDAFA nor the CFAA requires an invitation to visit an address accessible "to anyone with an Internet connection." (*hiQ Labs v. LinkedIn Corp.* (9th Cir. 2019) 938 F.3d 985, 1002 ("*hiQ Labs*"); see *infra*, Parts II–III.) At the threshold, though, it bears emphasizing that adopting the City's view of either statute would punish routine newsgathering and raise serious constitutional concerns.

The City's experience is not exceptional. Website operators routinely expose newsworthy information about themselves to the public, either without intending to or with the expectation that no one will notice. Just as routinely, journalists, academics,

and other researchers use a range of techniques to uncover and report that information in the public interest.

Take, for instance, web-scraping: the automated process of pulling large amounts of information from websites. Scraping typically does not expose any information beyond what could be found through the manual use of the website; its chief advantage is that it "speeds up the tedious job of manually copying and pasting data into a spreadsheet, making large-scale data collection possible." (Note, *Access Granted: A First Amendment Theory of Reform of the CFAA Access Provision* (2020) 120 Colum. L.Rev. 131, 137.) But the results, taken together, may reveal more than any one user visiting the website would have noticed.

Reporting of this kind has been used to expose grave public failings and unlawful private discrimination. (See, e.g., Zarkhin & 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> [as of Nov. 4, 2019]; Yachot, *Your Favorite Website Might Be Discriminating Against You* (June 29, 2016) ACLU <https://perma.cc/6W67-68J4> [as of Nov. 4, 2019].) Understandably, the subjects of stories like these would like the power to suppress them. As a result, websites now routinely

purport to forbid scraping, or otherwise using the information they host for research purposes, in their terms of service even as the information itself remains on public display. (See Note, *supra*, 120 Colum. L.Rev. at p. 134.) Like the City, they purport to tell journalists which information they may or may not gather on the open internet.

This view is unworkable. Private preferences cannot determine liability for routine, First Amendment newsgathering. If that were the case, subjects of journalistic investigations could simply decide to make such reporting unlawful. Consider the civil-rights testing and accountability journalism that inspired the 1988 amendments to the Fair Housing Act. (See Rottman, *Knight Institute's Facebook 'Safe Harbor' Proposal Showcases Need for Comprehensive CFAA Reform* (Aug. 6, 2018) Reporters Com. for Freedom of the Press <https://perma.cc/34C3-DJRE> [as of Oct. 31, 2019] [citing Dedman, *The Color of Money*, Atlanta Journal-Constitution (May 1–4, 1988)].) If conducted today, much of the data collection would take place through scraping and other online data journalism techniques. On the City's view, the subjects of such reporting could simply make such reporting illegal by invoking the CFAA and CDAFA. Not only would that

result chill reporting in the public interest, but also it would raise serious questions as to whether each law is void for vagueness—"unworkable and standardless"—because they make "each webmaster into its own legislature." (*Sandvig v. Barr* (D.D.C. 2020) 451 F.Supp.3d 73, 88 ("*Sandvig*").)

The City argues these broader interests are not at stake in this case. It argues that its Dropbox folder was never available for public scrutiny, as LinkedIn or Facebook is, because the URL was not referenced on the City's homepage. (Respondent's Br. 70–71.) The City cites no authority for the proposition that a resource deliberately published to the open internet remains "private" if the owner chooses not to advertise that information is hosted there. (See *infra*, Part II.) And this theory, too, threatens to chill routine journalism.

For instance, all major search engines allow users to use special commands called "operators" to conduct more efficient searches.[1] Investigative journalists often use these techniques to

[1] To offer a concrete example: Searching for "site:rcfp.org filetype:pdf" on Google will retrieve all of the PDF files that are hosted anywhere on the Reporters Committee's website, even though many are located at nonobvious URLs and would be difficult to find by clicking around. In fact, these files may be

find files that—while open to anyone who navigates to them—are not obviously accessible from an organization's main webpage. In one case, for example, a reporter's clever Googling revealed that a phone company had exposed reams of its customers' personal data "on unprotected Internet servers that anyone in the world could access," leading the Federal Communications Commission to launch its own investigation. (See Bowman, *FCC Announces $10 Million Fine for Security Breach Following Scripps Investigation* (Oct. 24, 2014) ABC Action News <https://bit.ly/2JMazaY> [as of Jan. 4, 2021].) The City's interpretation would outlaw that kind of reporting.

The City's position would likewise make it illegal for journalists and researchers to investigate even whether the use of nonobvious URLs is an adequate approach to maintaining the privacy of a webpage. Researchers and reporters have helped demonstrate that, at least in some settings, it is not. In 2016, for instance, a team of academics discovered they could access files users had hosted on Microsoft's cloud offering, OneDrive, by generating and automatically scanning millions of random

---

surfaced even if there is *no* live link to them, so long as they were indexed by Google at some earlier point in time.

shortened URLs. (See Greenberg, *Researchers Crack Microsoft and Google's Shortened URLs to Spy on People* (Apr. 14, 2016) Wired <https://perma.cc/984K-2PN4> [as of Oct. 16, 2020].) Microsoft fixed the issue after it was identified. (See Shmatikov, *Gone in Six Characters: Short URLs Considered Harmful for Cloud Services* (Apr. 14, 2016) Freedom to Tinker <https://perma.cc/3C82-TVP4> [as of Oct. 16, 2020].) By the City's lights, rather than fix the problem, a similarly situated company could have threatened litigation in an attempt to suppress disclosure of the flaw.

In sum, the City's interpretation of the CFAA and CDAFA threatens to criminalize a wide range of ordinary journalistic practices that serve the public interest without offering any safe harbor for reporters' First Amendment activities. But, this Court need not resolve the constitutional validity of the statutes raised by the City's interpretation here; it need only undertake a "narrow inquiry" into whether one reading of the statute "presents a significant risk" that a constitutional right "will be infringed." (*NLRB v. Catholic Bishop of Chicago* (1979) 440 U.S. 490, 502 [99 S.Ct. 1313, 59 L.Ed.2d 533].) To address just such First Amendment concerns, other courts have concluded that the

CFAA should be read to prohibit only the circumvention of certain code-based restrictions—not the violation of site owners' private expectations. (See, e.g., *Sandvig*, *supra*, 451 F.Supp.3d at pp. 88–89.) As between "plausible statutory constructions," if one "would raise . . . constitutional problems, the other should prevail." (*Clark v. Martinez* (2005) 543 U.S. 371, 380–81 [125 S.Ct. 716, 160 L.Ed.2d 734].) Thus, this Court should construe the CFAA and CDAFA narrowly to avoid this risk to lawful newsgathering in the public interest. (See *infra*, Parts II–III.)

II. The CFAA does not prohibit accessing information that a website owner has chosen to make available to any internet user.

To be clear, the CFAA does not, in fact, criminalize routine newsgathering. Instead, when Congress prohibited "access[ing] a computer without authorization," (18 U.S.C. § 1030(a)), it intended to prohibit conduct "analogous to . . . 'breaking and entering,'" (H.R.Rep. No. 98-894, 2d Sess., p. 20 (1984)). That is, it prohibited "hacking." (*hiQ Labs*, *supra*, 938 F.3d at p. 1000; see also, e.g., *United States v. Thomas* (5th Cir. 2017) 877 F.3d 591, 596 [noting the statute has an "antihacking purpose"].) Hacking is not what happened here.

The City appears to make at least three separate arguments to support its argument that Appellants should or "would have known" that they were not authorized to access the files at issue. (Respondent's Br. 62.) Each is based on a misunderstanding of ordinary norms of internet use. (Cf. Kerr, *Norms of Computer Trespass* (2016) 116 Colum. L.Rev. 1143, 1162 ["The first step in applying computer trespass law to the Web is to identify the nature of the space that the Web creates"].) More fundamentally, though, actual notice that a website owner does not appreciate a user's access is not enough to trigger liability under the CFAA, and the City's proffered theories to the contrary highlight the pitfalls of adopting such an approach. (See *hiQ Labs*, *supra*, 938 F.3d at pp. 1001–02.)

First, Respondent argues Appellants should have known the folder was private because the link to it was not featured on the City's website. (See Respondent's Br. 66.) To the Reporters Committee's knowledge, no court has held that access to a webpage is "without authorization" simply because its URL is nonobvious. (Contra Kerr, *supra*, 116 Colum. L.Rev. at pp. 1164–65 ["A hard-to-guess URL is still a URL, and the information posted at that address is still posted and accessible to the world"];

cf. *United States v. Morel* (1st Cir. 2019) 922 F.3d 1, 10–11 & fn. 9 [defendant had no reasonable expectation of privacy in images hosted at a URL "composed of random numbers and letters" because the URL was nevertheless accessible to anyone who stumbled across it].) This is for a good reason: It is difficult, if not impossible, for a user to know if a URL is "nonobvious" from the website owner's perspective. There are any number of ways to arrive at example.org/hypothetical-address-85910 without starting from example.org and clicking around (for instance, by using a search engine, as discussed *supra,* Part I). As a result, visitors to a specific URL have no way of knowing in the abstract if it was "private" in the sense the City claims.

Second, Respondent argues that Appellants should have known that they were only being given permission to access specific subfolders within the top-level folder because, in previous interactions, the "requester was *also* provided with the *specific name* of the subfolder containing the responsive public records." (See Respondent's Br. 21, original italics.) This is much like saying the City handed Appellants a folder full of documents and said, "The document we talked about before is located on page 16." Presumably, a person handed such a folder would conclude

she could look at the other pages, making a reasonable assumption that the folder would not contain information that was off-limits. The same is true in the cloud storage context. Because an account holder *can* use technical measures to share just one document, or just one subfolder, someone who is given access to an entire account reasonably understands that the owner did not intend to impose limits on access sub silentio.

Third and finally, Respondent argues that Appellants should have known that they could not access .zip folders in the Dropbox account that could be unzipped with a password. But not every field in a computer program labeled "password" is actually used, in context, to sort out unauthorized and authorized users. (Cf. Kerr, *supra*, 116 Colum. L.Rev. at p. 1173, fn. 153 [giving the example of a website that "required users to enter a secret password to enter the site but announced that the password was either 'red' or 'green'"].) Here, the City supplied Appellants and other public record requesters with generic passwords ("Fullerton!" or "Full3rtOn!") to unzip files responsive to their requests, (see Appellants' Br. 19), "passwords" that the City reused across folders, (see Respondent's Br. 22). By doing so, the City had effectively communicated to requesters,

including Appellants, that they could use the generic "password" whenever they needed to unzip a folder they had been given the ability to download. Having impliedly authorized that access, the City cannot rely on silent caveats to punish access after the fact. In sum, none of the conduct at issue goes against existing norms of internet use and none constitutes hacking that would violate the CFAA.

III. The CDAFA does not prohibit accessing information that a website owner has chosen to make accessible to any internet user.

The CDAFA, like the federal CFAA, is and should be about hacking. The trial court erred on that point, concluding that California Penal Code section 502 requires only proof of knowing *access* without permission—whether or not the defendant *knows* that his access is not permitted—and not proof of a technical intrusion. The court below based that conclusion entirely on a brief passage in the Ninth Circuit's opinion in *Facebook, Inc. v. Power Ventures, Inc.* (9th Cir. 2016) 844 F.3d 1058 ("*Power Ventures*"), setting up a distinction between the state law's prohibition on access "without permission" and the federal law's prohibition on access "without authorization," (*id.* at p. 1069). As a federal court opinion construing state law, it is not an

authoritative reading of the CDAFA. And, in any event, *Power Ventures* is distinguishable in a way that makes it poor support for the City's position.

California courts have often interpreted section 502 to require true "hacking." By its terms, the statute 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." (Cal. Pen. Code, § 502, subd. (c)(2).) "Access," in turn, is defined to mean "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." (*Id.,* § 502, subd. (b)(1), italics added.) As one of the leading appellate cases puts it, this definition is "redolent of 'hacking' or breaking into a computer." (*Chrisman v. City of Los Angeles* (2007) 155 Cal.App.4th 29, 34 [65 Cal.Rptr.3d 701].)

In *Chrisman*, the court of appeal went on to reject the application of section 502 to a police officer who made personal use of a law enforcement database 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.'"[2] (*Id*. at p. 35.) The court explained that section 502 does not apply to the "ordinary, everyday use of a computer," including "improper computer inquiries" by an individual who already has access to a database. (*Id*. at pp. 34–35.) By comparison, in *People v. Childs* (2013) 220 Cal.App.4th 1079, 1105 [164 Cal.Rptr.3d 287], the court of appeal found that section 502 *did* apply to a system administrator who coded a government computer system to lock out users and delete data if others tried to access it, contrasting his actions with "routine" computer misuse. A similar distinction between unknowing frustration of a site owner's unarticulated expectations and technical interference is decisive here.

Power Ventures is not to the contrary. For one, as a federal case interpreting state law, the opinion is not authoritative.[3]

---

[2] Of course, misuse of government databases by public employees can be made a punishable offense—but it is not a general "computer crime."

[3] The City invokes *United States v. Christensen* (9th Cir. 2015) 828 F.3d 763, to the same effect. But *Christensen* has never been cited, let alone applied, by any California court of appeal. Moreover, the Ninth Circuit in *Christensen* explicitly acknowledged that section 502 is susceptible of the interpretation

Even on its own terms, though, the decision is inapposite. There, the court concluded that the defendants violated California's statute because they continued to access information after the plaintiff had made an explicit request for them to stop. (See *Power Ventures*, *supra*, 844 F.3d at p. 1069.) Here, by comparison, Respondent argues that Appellants violated section 502 by accessing files available to anyone on the internet in the absence of *affirmative* permission. Fair notice concerns are less acute when, as in *Power Ventures*, the user has been asked to stop doing what she is doing; they are at their height where, as here, the user is asked to infer that access is forbidden even though a site's owner has chosen to make access possible.

---

adopted in *Chrisman*: i.e., that "knowing access" requires proof of activity that resembles hacking. (*Id.* at p. 789.)

CONCLUSION

For all of these reasons the Reporters Committee urges this Court to vacate the preliminary injunction.

Respectfully submitted,

/s/

Katie Townsend
(SBN 254321)
Counsel of Record for Amicus Curiae
Bruce D. Brown**
Gabriel Rottman**
REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS
***Of counsel*

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 Century Schoolbook font type, including footnotes, and contains 3,913 words. I have relied on the word-count function of the Microsoft Word word-processing program used to prepare this brief.

Dated: January 4, 2021

/s/ Katie Townsend
Katie Townsend
Counsel of Record for Amicus Curiae
Bruce D. Brown**
Gabriel Rottman**
** *Of counsel*

PROOF OF SERVICE

I, Katie Townsend, 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 Street NW, Suite 1020, Washington, D.C. 20005. I am a citizen of the United States and am employed in Washington, District of Columbia.

On January 4, 2021, I caused the foregoing documents to be served: **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 Appellants**, 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:

The Superior Court of Orange County : Respondent
Hon. James L. Crandall Dept. C33
700 Civic Center Dr West
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 January 4, 2021, in Washington, D.C.

By: */s/ Katie Townsend*
Katie Townsend
Counsel of Record for Amicus Curiae