Case No.: G058996

IN THE COURT OF APPEAL FOR THE STATE OF CALIFORNIA
FOURTH APPELLATE DISTRICT, DIVISION THREE

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

Appellants,

v.

CITY OF FULLERTON,

Respondent.

On appeal after issuance of a preliminary injunction
and denial of anti-SLAPP motion
Case No. 30-2019-01107063

Appeal from the Superior Court for Orange County
The Honorable James L. Crandall

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA IN SUPPORT OF APPELLANTS

Peter Bibring (SBN 223981)
Mohammad Tajsar (SBN 280152)
ACLU FOUNDATION OF SOUTHERN CALIFORNIA
1313 West Eighth Street
Los Angeles, California 90017
T: (213) 977-5295
F: (213) 915-5297

Mark Rumold (SBN 279060)
Andrew Crocker (SBN 291596)
Aaron Mackey (SBN 286647)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
T: (415) 436-9333
F: (415) 436-9993
mark@eff.org

Counsel for Amici Curiae

Additional counsel on next page

Brett Max Kaufman
Esha Bhandari
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Fl.
New York, NY 10004
T: (212) 549-2500
F: (212) 549-2652

Jennifer Stisa Granick (SBN 168423)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
T: (415) 343-0758
F: (415) 255-1478

CERTIFICATE OF INTERESTED PARTIES

Pursuant to California Rules of Court 8.208, the Electronic Frontier Foundation states that it is a non-profit, non-partisan civil liberties organization. EFF has no parent corporation and no publicly held corporation owns 10% more of its stock.

Pursuant to California Rules of Court 8.208, ACLU and ACLU of Southern California state that they are non-profit, non-partisan civil liberties organizations. ACLU and ACLU of Southern California have no parent corporation and no publicly held corporation owns 10% more of their stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Legislative Materials

Other Authorities

INTRODUCTION

The City of Fullerton stored documents online that were accessible to any Internet user in the world. When Appellants Joshua Ferguson and David Curlee—contributors to the local news blog, *Friends for Fullerton's Future*—obtained those documents, they did what journalists do: they re-published them, along with commentary and analysis.

Nothing about that conduct is unusual—much less illegal. Journalists regularly comb websites for data or investigative scoops the general public might otherwise miss. Indeed, for reporters, this type of online investigation is among "the most powerful techniques for data-savvy journalists who want to get the story first, or find exclusives that no else has spotted."[1]

What *is* unusual is the City's response. Rather than accept responsibility for its own failure to limit public access to information, the City instead is attempting to stretch computer crime laws to punish those journalists—first, for uncovering unflattering information and, later, for publishing it. The Court should reject this misguided effort to twist criminal law to punish truthful reporting. Adopting the City's arguments will chill those who report on government affairs, both in the City of Fullerton and throughout California.

As explained below, the Superior Court incorrectly granted the

[1] Paul Bradshaw, *Scraping for Journalists* (2d ed. 2017) (ebook), https://leanpub.com/scrapingforjournalists.

City's preliminary injunction. This Court should reverse it.

FACTUAL BACKGROUND

Several years ago, the City began using Dropbox to facilitate the review and distribution of City documents to members of the public, including documents made public pursuant to Public Records Act requests. 1 Appellants' Appendix ("AA") 106 ¶¶ 6–7; 1 AA 140 ¶ 20.

Dropbox is a third-party, cloud-based application that helps users store and share data. The City chose www.cityoffullerton.com/outbox ("outbox URL")[2] as the address for its Dropbox account. 2 AA 731 ¶ 21. That choice made the City's Dropbox page appear as though it were an integrated part of the City's website, www.cityoffullerton.com. The outbox URL is intuitive, easy to remember, and easy to guess.

The City chose not to require a username or password to access the outbox URL. 2 AA 731–32 ¶¶ 22–23. There were no password restrictions limiting access to particular folders in the account, *see, e.g.*, 2 AA 729–31, 747–49; nor was a password required to download files from the Dropbox account. *See* 2 AA 748.

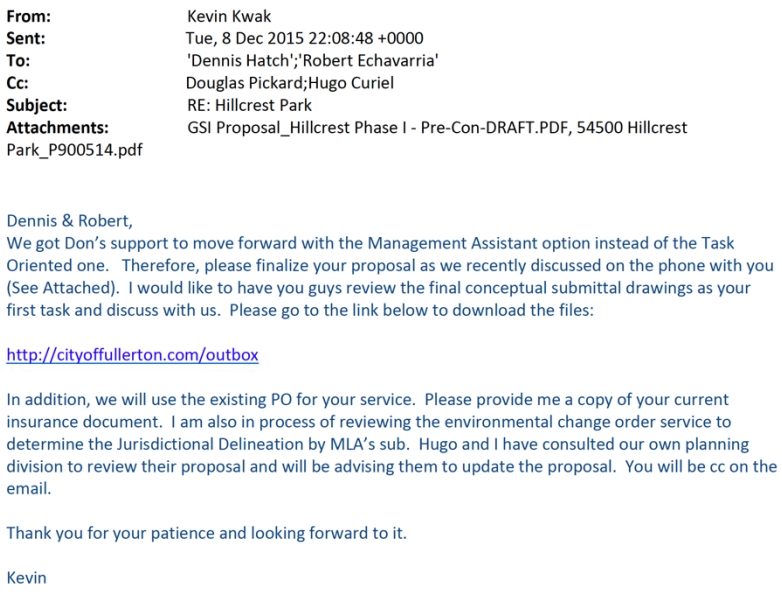
As a result of the setup options the City selected, any Internet user could enter the outbox URL into a web browser and (1) access the entire

[2] A URL, or Uniform Resource Locator, is "the address of a resource (such as a document or website) on the Internet." *Definition of URL*, Merriam-Webster, https://www.merriam-webster.com/dictionary/URL.

contents of the City's Dropbox storage and (2) download any file stored there. 2 AA 731 ¶ 20. In other words, the stored documents were publicly accessible on the Internet to any person in the world.

While the documents the City stored in its Dropbox had unique names and links, all those documents and links were publicly available through the outbox URL. A unique link was not required to access specific documents once a user navigated to www.cityoffullerton.com/outbox.

The record demonstrates that the City regularly shared the outbox URL in the course of City business. For example, City employees provided the outbox URL to various companies—architects, engineering firms, and contractors—in email correspondence with the City's Public Works Departments, as shown in the image below:



From: Kevin Kwak
Sent: Tue, 8 Dec 2015 22:08:48 +0000
To: 'Dennis Hatch';'Robert Echavarria'
Cc: Douglas Pickard;Hugo Curiel
Subject: RE: Hillcrest Park
Attachments: GSI Proposal_Hillcrest Phase I - Pre-Con-DRAFT.PDF, 54500 Hillcrest Park_P900514.pdf

Dennis & Robert,
We got Don's support to move forward with the Management Assistant option instead of the Task Oriented one. Therefore, please finalize your proposal as we recently discussed on the phone with you (See Attached). I would like to have you guys review the final conceptual submittal drawings as your first task and discuss with us. Please go to the link below to download the files:

http://cityoffullerton.com/outbox

In addition, we will use the existing PO for your service. Please provide me a copy of your current insurance document. I am also in process of reviewing the environmental change order service to determine the Jurisdictional Delineation by MLA's sub. Hugo and I have consulted our own planning division to review their proposal and will be advising them to update the proposal. You will be cc on the email.

Thank you for your patience and looking forward to it.

Kevin

2 AA 752; *see also id.* at 751 (same); 754–55 (same); 758–63 (same); 765 (same).

The City used the outbox URL in a second way: it provided the outbox URL to members of the public (including one of the journalists here) to facilitate the production of records in response to public records requests, as shown in the image below:

From: Margot Cronce
To: David Curlee
Cc: Claire Moynihan; Mea Klein; Susana Barrios
Subject: RE: Pro-card statements
Date: Thursday, June 6, 2019 4:10:46 PM
Importance: High

Hi David,
The zipped file for the pro card statements has been placed in the drop box.
The **file name** is: **PRR Pro Card 5-29-19**
Here's the **link: http://cityoffullerton.com/outbox**

The **password** to unzip the file is: **Full3rt0n!**
Please let me know if you have any problems retrieving the file.
Thank you,
Margot Cronce I Purchasing Manager I City of Fullerton
303 W. Commonwealth Avenue I Fullerton CA 92832
Ph: 714/738-6535 I Fax: 714/738-3168 I margotc@cityoffullerton.com

1 AA 123 (email to appellant Curlee); *see also* AA 115.

Finally, the outbox URL was disseminated in a third way: the City disclosed the outbox URL in Public Records Act *productions*. *See, e.g.*, 1 AA 747 ¶¶ 6–7. That is, not only did the City use and share the outbox URL, via email, in the course of City business; but it then produced those emails in response to Public Records Act requests from members of the public. By disclosing the outbox URL, without redaction, as part of a public record, the outbox URL was presumptively information "relating to the conduct of the public's business" in California. *See* Cal. Gov. Code § 6252(e).

ARGUMENT

California's Comprehensive Computer Data Access and Fraud Act, Penal Code § 502 ("Section 502"), does not prohibit the conduct alleged here. Like its federal counterpart, the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, Section 502 was intended to criminalize malicious computer intrusions—not the type of online access to publicly available information that occurred here. The City's interpretation of Section 502 goes well beyond how other courts have defined the type of "hacking" proscribed by the statute. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1001–02 (9th Cir. 2019) (because website was "available to anyone with an Internet connection," it constituted "information for which access is open to the general public and permission is not required").

Additionally, principles of constitutional avoidance require that these statutes be interpreted narrowly. Similar to its federal counterpart, several key terms in Section 502 are dangerously vague and, if misconstrued, could create civil and criminal liability for a wide swath of common and innocuous online behavior. Interpreting Section 502 as broadly as the City demands would violate the First Amendment and Due Process.

I. Section 502 Does Not Prohibit Accessing Data Stored Online that Is Available to Any Internet User in the World.

Section 502, which creates a "laundry list" of criminal and civil penalties for various computer crimes, does not criminalize access to online information available to anyone with an Internet connection. *See People v. Lawton*, 48 Cal.App.4th Supp. 11, 15 (1996); Cal. Penal Code § 502.

Instead, Section 502 creates liability for one who "[k]nowingly accesses and without permission takes . . . data from a computer." § 502(c)(2). In addition to civil penalties, *see* § 502(e)(1), violations of this provision constitute a felony, punishable by imprisonment for up to three years and a fine up to $10,000. § 502(d)(1).

The City's brief focuses largely on the statute's requirement of "knowing[] access," Resp't Br. at 47, 50, but that focus is misplaced. The requirement of "knowing[]" access distinguishes between intentional and inadvertent accesses. *See People v. Hawkins*, 98 Cal.App.4th 1428, 1438 (2002). Here, there is no suggestion of any *inadvertent* access.

The only relevant question in this case is whether the journalists accessed data—the various documents and files allegedly downloaded from the City's Dropbox storage—"without permission." *See* § 502(c)(2).[3]

[3] The statute's *mens rea* requirement—"knowingly"—applies to knowing one is accessing data without permission. *Hawkins*, 98 Cal.App.4th at 1437–38 (applying "knowingly" *mens rea* requirement to "without permission"). But here, there was no permission required. Section I.B, *infra*.

The City contends that journalists act "without permission," and thus *commit a crime* under Section 502, by accessing a particular City-controlled URL and downloading documents stored there—notwithstanding the fact that the URL is in regular use in City business and has been disseminated to the general public. The City claims that an individual may access a publicly available URL, and download documents stored in a publicly accessible account, only if the City specifically provides that URL in an email addressed to that particular person. But that interpretation of "permission" produces absurd—and dangerous—results: the City could choose arbitrarily to make a criminal of many visitors to its website, simply by claiming that it had not provided the requisite permission-email to the visitor.[4]

The City further claims that its use of a unique and difficult-to-guess link for a document means only specific individuals receiving that link have permission to access the document. Resp't Br. at 16–17, 70. But the City was using the outbox URL, in some cases, to make public documents it was

[4] For example, the City states: "a *violation* of Section 502 occurs when any person merely '[k]nowingly accesses' the government's computer data. Cal. Penal Code § 502 (c)(2). Thus, there is *no* requirement that there be any breaking into a computer system, any bypassing or even the presence of any security features, nor any fraudulent or malicious intent." Resp't Br. at 50. The City's interpretation of Section 502 is untenable. Under the City's articulation of the rule, a person could be liable for violating Section 502 *anytime* they visited the City's website if the City disapproves of their access.

required by law to disseminate under the Public Records Act. 1 AA 106, 108, 109, 123; 2 AA 727, 747–48, 751–65. "Every person has a right to inspect" these public records, regardless of the structure of the link. Cal. Gov. Code § 6253(a). Criminal liability cannot and does not turn on the subjective whims of website owners. *See United States v. Nosal* ("*Nosal I*"), 676 F.3d 854, 859–62 (9th Cir. 2012) (en banc) (warning that a holding to the contrary means that "millions of unsuspecting individuals" could "find that they are engaging in criminal conduct").

Instead, "permission" on the Internet, for purposes of Section 502 liability, is defined through technical access controls—like login credentials, or other technical measures taken to grant certain users access and to prohibit access by other users. *See Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026, 1032 (N.D. Cal. 2014). Where no technical barriers exist and websites are accessible by the public, "permission" to access data is simply "not required." *See hiQ Labs*, 938 F.3d at 1001.

This interpretation of "permission"—one that, at minimum, is regulated through technical access controls—reflects the longstanding open-access norms of the Internet. *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1161 (2016). For this reason, the City's repeated comparisons to the physical world badly miss the mark. *See, e.g.*, Resp't Br. at 23–24 (analogizing situation to "one [who] accidentally leaves a house or car door unlocked—or even wide open").

Absent technical barriers, the Internet is "inherently" and "presumptively" open for all, unlike a private home with an open door. Kerr, *Norms of Computer Trespass* at 1161.

Here, Appellants did not bypass any technical barriers in accessing the City's Dropbox account or in downloading files from that account. Accordingly, there can be no liability under Section 502.

A. Interpreting "Without Permission" to Require the Circumvention of Technical Access Controls Is Consistent with Section 502's Legislative History and Other Cases Interpreting the Statute.

Interpreting "without permission" to require, at minimum, the circumvention or bypassing of some type of technical access barrier is consistent with Section 502's legislative purpose and cases that have interpreted the statute.

In *Chrisman v. City of Los Angeles*, 155 Cal.App.4th 29 (2007), the Court of Appeal recognized that a primary legislative purpose of Section 502 is to deter computer hackers—those "outsiders who *break into a computer system* to obtain or alter the information contained there." *Id.* at 34 (quoting *People v. Gentry*, 234 Cal.App.3d 131, 141 n.8 (1991)) (emphasis added). The *Chrisman* court contrasted that type of "hacking," which is prohibited by Section 502, with accessing data for a purpose, or in a manner, unapproved by the computer owner—conduct beyond the statute's reach. 155 Cal.App.4th at 34-35.

Indeed, a series of federal courts have recognized that a person acts "without permission" within the meaning of Section 502 only when they "circumvent[] technical or code-based barriers in place to restrict or bar a user's access." *Sunbelt Rentals*, 43 F. Supp. 3d at 1032 (quoting *Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1036 (N.D. Cal. 2012)); *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 950 (N. D. Cal. 2014) (same); *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043 (N.D. Cal. 2018) (same); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 716 (N.D. Cal. 2011) (same).

B. Section 502 Should Be Interpreted Similarly to the CFAA, Which Does Not Prohibit the Conduct Alleged Here.

Given the similar purposes shared by Section 502 and its federal counterpart, the CFAA, the statutes should be given similar reach. Indeed, courts recognize that, "despite differences in wording, the analysis under both statutes is similar" in cases where no technical barriers to accessing data exist. *Facebook, Inc. v. Power Ventures* ("*Power Ventures*"), 844 F.3d 1058, 1069 (9th Cir. 2016); *hiQ Labs*, 938 F.3d at 1000–01 (affirming preliminary injunction against enforcement of CFAA and Section 502 because permission was "not required" to access website without technical barriers).

The CFAA, like Section 502, was primarily intended to prohibit computer hacking. *See Nosal I*, 676 F.3d at 858 (citing S. Rep. No. 99-432,

at 9 (1986) (Conf. Rep.). And both statutes rely on similar operative terminology—under the CFAA, "without authorization," 18 U.S.C. § 1030(a)(2)(C), and, under Section 502, "without permission." *See United States v. Nosal* ("*Nosal II*"), 844 F.3d 1024, 1028 (9th Cir. 2016) (holding "'without authorization' is an unambiguous, non-technical term" that means "without permission"); *see also* Black's Law Dictionary (10th ed. 2014) (defining "authorization" as "[o]fficial permission").

Access to a public website does not constitute a violation of the CFAA. This is because the CFAA was enacted as "an anti-intrusion statute" to prevent serious computer hacking. *hiQ Labs*, 938 F.3d at 1000–01 (reviewing legislative history).

Where information is publicly available to any Internet user—like the documents at issue here—courts recognize that *everyone* using the Internet is "authorized" to access the data. *See, e.g., id*. at 1000, 1003; *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011) (the public is presumptively authorized to access an "unprotected website"); *Craigslist, Inc. v. 3Taps, Inc*., 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013) (making a website publicly available gives everyone "authorization" to view it under the CFAA). Indeed, even a cease and desist letter cannot render access to publicly available websites "without authorization." *hiQ Labs*, 938 F.3d at 1002 (*Power Ventures* "do[es] not control the situation present here, in which information is

'presumptively open to all comers.").

The Ninth Circuit's decision in *hiQ Labs* lays to rest any argument that Appellants violated the CFAA in accessing the City's Dropbox storage because the storage was somehow "not public." *See* Resp't Br. at 17, 65 (disputing the description of Dropbox as "public" because it was not linked from the City's main website). In *hiQ Labs*, hiQ, a data analytics company, used an automated tool to collect information from publicly accessible LinkedIn profiles, which LinkedIn alleged violated the CFAA. The court disagreed, writing that "authorization is only required for password-protected sites or sites that otherwise prevent the general public from viewing the information." 938 F.3d at 1001. Because the LinkedIn profiles were "available to anyone with an Internet connection," they constituted "information for which access is open to the general public and permission is not required." *Id.* at 1001–02. LinkedIn did not explicitly link to or direct hiQ to public user profiles,[5] yet the court found them to be public because they could be accessed without any permission requirement. Thus, a website operator need not *publicize* a website in order for it to be *public* in the relevant legal sense.[6]

[5] hiQ accessed LinkedIn profiles using a "bot," akin to the web crawlers employed by Google and other search engines to "systematically search[] the Internet and download[] copies of web pages, which can then be indexed by a search engine." *Id.* at 990 n.2.

[6] *Harleysville Ins. Co. v. Holding Funeral Home, Inc.*, No. 15-cv-00057, 2017 WL 4368617, at *8 (W.D. Va. Oct. 2, 2017), relied on by the City,

Here, the City's Dropbox was similarly publicly accessible, without a password or other permission requirement, and "available to anyone with an Internet connection." *Id.* at 1002. It is thus irrelevant that the City argues it did not publicize a link to the account from the City's main website. The City could have indicated who was and was not authorized to access its Dropbox account by implementing some form of technical access barrier—like a username and password to access either the account as a whole, or by more granularly requiring a password to access particular folders or download particular files within the account. *See id*. at 1001 (quoting Kerr, *Norms of Computer Trespass* at 1161 ("An authentication requirement, such as a password gate, is needed to create the necessary barrier that divides open spaces from closed spaces on the Web.")). Indeed, Dropbox offers all these capabilities. *See* 2 AA 727–30 (Bambenek Decl. ¶¶ 13–18).

Implementing some type of authentication requirement would have allowed the City to let authorized users in and keep unwanted individuals out. But—whether intentionally or inadvertently—the City did not implement any technical access barrier. It left its account wholly available to any Internet user and affirmatively shared the account's URL with members of the public, who in turn were free to share the URL with other

---

does not involve the CFAA (or similar anti-hacking statutes such as Section 502). Thus, that case's discussion of whether a cloud filesharing service without password protection is public is inapposite.

members of the public. *See supra* Factual Background 7–8 (describing ways in which outbox URL was disseminated).

The *hiQ Labs* decision also demonstrates why the City cannot rely on cases such as *Power Ventures* and *United States v. Christensen*, 828 F.3d 763 (9th Cir. 2016). *Power Ventures* involved CFAA and Section 502 claims brought by Facebook against Power, a social media aggregator that accessed Facebook users' accounts with the users' consent. The Ninth Circuit held that Power had "implied authorization" to access Facebook's computers until Facebook revoked this authorization in a cease and desist letter to Power. 844 F.3d at 1069. However, in *hiQ Labs*, the court explained that *Power Ventures* only applies to "situations in which authorization generally is required and has either never been given or has been revoked." 938 F.3d at 1002. It does not apply in situations, like this case, where "information is 'presumptively open to all comers.'" *Id.* (quoting *Power Ventures*, 844 F.3d at 1067 n.2).

Thus, without password protection or other measures taken to "prevent the general public from viewing" its Dropbox folder, the City cannot rely on *Power Ventures* to differentiate its Section 502 claim from its unsupported CFAA claim. *Id.* at 1001; *see also hiQ Labs v. LinkedIn Corp.,* 273 F. Supp. 3d 1099, 1115 n.13 (N.D. Cal. 2017) (concluding that Section 502 likely did not apply and noting "there are serious questions about whether these provisions criminalize viewing public portions of a

website").

The same is true for *Christensen*, which held "access" as used in Section 502 includes "*logging into a database* with a valid password and subsequently taking, copying, or using the information in the database improperly." 828 F.3d at 789 (emphasis added). *See* Resp't Br. at 47–48 (citing *Christensen*, 828 F.3d at 789; *Satmodo, LLC v. Whenever Commc'ns, LLC*, No. 17-cv-0192, 2017 WL 6327132 (S.D. Cal. Dec. 8, 2017)).[7] Appellants here did not log in to the City's Dropbox account—because no login was required—and hence cannot have violated Section 502 in the manner discussed in these cases.[8]

II. Section 502 Must Be Construed Narrowly to Protect Journalists and to Avoid Conflict with the State and Federal Constitutions.

Section 502's text and statutory purpose are determinative: obtaining data from a publicly available website is not a crime. And the host of constitutional problems presented by the City's proposed interpretation of Section 502 reinforce that result.

---

[7] Additional cases relied on by the City similarly turn on the use of valid log-in information for improper purposes. *See NovelPoster v. Javitch Canfield Grp.,* 140 F. Supp. 3d 954, 967 (N.D. Cal. 2014) (claim that defendant "used technically-operable log-in information to access portions of a computer system which the individual knew he was not permitted to access"); *DocMagic v. Ellie Mae*, 745 F. Supp. 2d 1119, 1151 (N.D. Cal. 2010) (claim based on repeated use of third parties' login credentials).

[8] Some files stored in the City's Dropbox account were compressed (or "zipped" files) and required a password to unzip. These files, like all others in the City's Dropbox, were free and available to download to the user's

The City's broad interpretation of Section 502 would criminalize—and undoubtedly chill—valuable newsgathering and would violate the California and United States Constitutions in several respects. When a court is confronted with two potential interpretations of a statute and "one of them would create a multitude of constitutional problems, the other should prevail." *Clark v. Martinez*, 573 U.S. 371, 380-81 (2005).

A narrow interpretation of Section 502 must prevail here. The City's construction of Section 502 creates significant risks to the exercise of First Amendment rights and incurable Due Process concerns. The City's interpretation would permit public officials to decide—after making records publicly available online (through their own fault or otherwise)—that accessing those records was illegal. Under the City's theory, it can retroactively revoke generalized permission to access publicly available documents as to a single individual or group of users once it changes its

---

own computer without a password. However, in some circumstances, a password was then required to decompress and open the files on the user's own computer. The process of unzipping a file on a user's own computer does not implicate the CFAA because that statute does not reach subsequent use of data that was accessed with authorization. *Nosal I*, 676 F.3d at 863. Meanwhile, although Section 502 may encompass subsequent use of data "without permission," the burden is on the plaintiff to demonstrate that use was unpermitted. The City has not demonstrated that the Appellants unzipped any files without permission. Indeed, on at least two occasions, the City provided a password to decompress files directly to Appellants. *See* 1 AA 115, 123.

mind or is simply embarrassed by the documents' publication. The City could then leverage that revocation of permission into a violation of Section 502 and pursue both civil and criminal liability against the parties who accessed the materials. If that were the law, members of the public who accessed City records online could rarely be confident that they had lawful access to those records.

The concern about public officials using unchecked discretion to target members of the public under Section 502 is not hypothetical: It is the apparent purpose of the City's use of Section 502 here. Indeed, the City's real concern appears to be not how the documents were accessed but that the documents were *published*. The Court need look no further than the City's conduct here to appreciate the very real constitutional problems presented by an expansive interpretation of Section 502.

Faced with similarly broad arguments, courts have relied upon the canon of constitutional avoidance to narrowly interpret the CFAA in order to avoid creating significant risks to individuals' First Amendment and Due Process rights. *See Sandvig v. Barr* 451 F. Supp. 3d 73, 88–89 (D.D.C. 2020), *appeal docketed*, No. 20-5153 (D.C. Cir. May 28, 2020) ("Plaintiffs' First Amendment challenge raises such risks . . . and thus weighs in favor of a narrow interpretation under the avoidance canon."); *Nosal I*, 676 F.3d at 863 (construing the CFAA narrowly "so that Congress will not unintentionally turn ordinary citizens into criminals").

For essentially the same reasons, this Court should impose a narrow interpretation on Section 502.

A. Section 502's Language Should Be Interpreted Narrowly Because a Broad Interpretation Would Chill First Amendment–Protected Activity.

The City's broad reading of Section 502 would chill socially valuable research, journalism, and online security and anti-discrimination testing—activity squarely protected by the First Amendment.

To give just one example, the City's interpretation could criminalize—and therefore will undoubtedly chill—a specific category of online activity that is critically important to holding companies accountable: the investigative techniques employed by journalists and academic researchers to uncover online discrimination. These techniques sometimes involve violating contractual prohibitions on certain online activities, and the research these journalists or academics conduct is often adversarial to public officials or a company's business interests.

Online, there is growing evidence that proprietary algorithms are causing websites to discriminate among users, including on the basis of race, gender, and other characteristics protected under civil rights laws.[9] To uncover whether any particular website is treating users differently,

[9] *See, e.g.*, Exec. Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* (May 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

researchers need to use a variety of techniques, such as creating test accounts that vary on the basis of race or gender and comparing the job ads or housing offers that are displayed to, say, male versus female users. In this case, researchers may need to access the accounts of actual users to compare housing or job offers that are given to people of different genders or races. Such techniques, which do not constitute hacking, are often adversarial to a company's interests.

Under the City's interpretation of Section 502, if a company disagrees with the purpose of a researcher's access to its website, it can not only seek to bar such research but can actually render that research criminal by either (1) stating in terms of use or by letter that researchers are not authorized to access its website,[10] or (2) later announcing that those individuals acted without permission.

Websites, including those maintained by California state agencies and local governments, could therefore rely on the criminal charges to shut down unwanted research or testing, even where the researcher did not hack into a computer. Under a broad interpretation of Section 502, the website owner's choice to prohibit such research could be enforceable as a criminal violation. As a result of that threat of criminal prosecution, many

[10] See, e.g., Knight First Amendment Inst., *Knight Institute Calls on Facebook to Lift Restrictions on Digital Journalism and Research* (Aug. 7, 2018), https://knightcolumbia.org/content/knight-institute-calls-facebook-lift-restrictions-digital-journalism-and-research.

researchers and journalists will likely refrain from conducting their socially valuable and constitutionally protected research.

The Court can avoid this outcome by rejecting the City's interpretation of "without permission."

B. Aside From Chilling Constitutionally Protected Activity, Interpreting "Without Permission" Broadly Would Lead to Unconstitutional Applications of Section 502.

In case there was any doubt that interpreting Section 502 broadly should be avoided, the statute cannot be applied to the journalists without creating a serious risk of violating the First Amendment.

The only way Appellants' access to the documents can be viewed as violating Section 502, and thus engaging in illegal activity, is by reading "without permission" to mean obtaining information that the City does not want to be public, even when the City placed that very information on publicly accessible websites. But the Supreme Court has recognized that "state action to punish the publication of truthful information seldom can satisfy constitutional standards." *Smith v. Daily Mail Publ'g Co.,* 443 U.S. 97, 102 (1979).

Appellants have a First Amendment right to publish the documents at issue because they are a matter of public concern. The First Amendment protects Appellants' publication of documents they obtained from the City, even when the City claims that such information is non-public or that a statute prohibits their disclosure. This First Amendment protection has

special force when the information at issue was obtained from the government, even if government officials erred in disclosing it and later claim the access was without permission. *See Florida Star v. B.J.F.,* 491 U.S. 524, 525 (1989) (reporter obtained victim's name from police report inadvertently placed in pressroom); *Daily Mail*, 443 U.S. at 98 (reporters learned juvenile suspect's name by asking police and a prosecutor at the crime scene); *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 495 (1975) (reporter learned victim's name by reviewing indictments made available in the courtroom).

The City attempts to sidestep these First Amendment problems by arguing that *Daily Mail* and its progeny do not apply to Appellants, but its argument is circular. According to the City, Appellants engaged in illegal activity by accessing the information and, thus, fall outside of the First Amendment's protections. Resp't Br. at 37–39. The City's argument thus requires expanding liability under Section 502 in ways that are antithetical to the very purposes of the First Amendment's protections articulated in *Daily Mail*: "A free press cannot be made to rely solely upon the sufferance of government to supply it with information." 443 U.S. at 104.

To interpret Section 502's "without permission" language so as to impose liability here, the City must show that its asserted interests in the documents are "of the highest order," that it has no other, less-intrusive means to protect the information, and that its use of Section 502 to penalize

Appellants is narrowly tailored to protecting those interests. *Id*. at 102–04; *Florida Star*, 491 U.S. at 533–540. First, the City has "far more limited means of guarding against dissemination than the extreme step of punishing truthful speech," *Florida Star*, 491 U.S. at 538, for example, using password protection on its Dropbox account. The City failed to use any more "limited means" to protect the information and instead seeks to expand Section 502 because it did not want the public to learn about the matters of public concern discussed in the documents. Second, "[w]here, as here, the government has failed to police itself in disseminating information," imposing civil liability on Appellants for their publication "can hardly be said to be a narrowly tailored means" of vindicating the interests the City claims in the documents. *Id*. Third, even granting the City's interest in protecting the confidentiality of records it traditionally has not made public, that interest is not sufficient to justify an interpretation of Section 502 that would create criminal and civil liability for any member of the public who clicks on a publicly available link to a City-controlled "outbox" and uses or publishes the information it finds there. *See Daily Mail*, 443 U.S. at 104 (recognizing that "[t]he magnitude of the State's interest" in enforcing a statute is not sufficient to justify criminal liability).

C. The City's Interpretation of "Without Permission" Renders Section 502 Unconstitutionally Vague.

The City's broad interpretation of Section 502's "without permission" language would also violate the Due Process clause. An average Internet user would not be on notice that, by accessing documents posted on a publicly available website, the user was acting "without permission" and, thus, committing a crime. The City's interpretation would thus render Section 502 unconstitutionally vague, a result the Court can avoid by interpreting the statute narrowly.

Due process requires that criminal statutes provide ample notice of what conduct is prohibited.[11] *Connally v. Gen. Const. Co*., 269 U.S. 385, 390 (1926). Vague laws that do not "provide explicit standards for those who apply them . . . impermissibly delegate[] basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis." *Grayned v. Rockford,* 408 U.S. 104, 108–09 (1972). A criminal statute that fails to provide fair notice of what is criminal—or threatens arbitrary and discriminatory enforcement—is thus void for vagueness. *Skilling v. United States*, 561 U.S. 358, 412 (2010) (citing *Kolender v.*

[11] Although here the City brings civil claims under Section 502, the statute's prohibitions against making use of computer data "without permission" are also criminal. Cal. Penal Code § 502 (c)(2). Due Process constraints on criminal statutes therefore apply to any interpretation of Section 502.

Lawson, 461 U.S. 352, 357 (1983)).

To avoid fatal vagueness problems, the rule of lenity calls for ambiguous criminal statutes to be interpreted narrowly in favor of the defendant. *United States v. Santos*, 553 U.S. 507, 514 (2008). The rule "ensures fair warning by so resolving ambiguity in a criminal statute as to apply [] only to conduct clearly covered." *United States v. Lanier*, 520 U.S. 259, 266 (1997). The rule of lenity "not only ensures that citizens will have fair notice of the criminal laws, but also that [a legislature] will have fair notice of what conduct its laws criminalize. We construe criminal statutes narrowly so that [a legislature] will not unintentionally turn ordinary citizens into criminals." *Nosal I*, 676 F.3d at 863.

Courts interpreting ambiguous provisions of the CFAA use the rule of lenity to avoid potential vagueness problems. This Court should follow suit to construe Section 502 narrowly.

Broad interpretations of computer crime statutes fail to give people adequate notice of criminal activity and vest far too much power and enforcement discretion in third parties and the government. Courts recognize that while the CFAA *could* be interpreted to base criminal liability based on subjective criteria—like website terms of service or computer-use policies instituted by an employer—such an interpretation would violate the rule of lenity by conferring on private parties the power to outlaw any conduct they wish without the clarity and specificity required

of criminal law. *See United States v. Valle*, 807 F.3d 508, 527 (2nd Cir. 2015); *WEC Carolina Energy Sols., Inc., v. Miller*, 687 F.3d 199, 205–06 (4th Cir. 2012); *Nosal I*, 676 F.3d at 860; *cf. Sandvig*, 451 F. Supp. 3d at 88 (narrowly interpreting the CFAA, including for lenity concerns, and noting that "[c]riminalizing terms-of-service violations risks turning each website into its own criminal jurisdiction and each webmaster into his own legislature.").

Specifically, "allow[ing] criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read" would create "[s]ignificant notice problems[.]" *Nosal I*, 676 F.3d at 860. Indeed, attaching criminal punishment to breaches of vague, boilerplate policies[12]—which companies typically reserve the right to modify at any time[13]—would make it impossible for individuals to know what conduct is

---

[12] One sample Internet and email usage policy, for example, warns that "Internet use on company time or using company-owned devices that are connected to the company network is authorized to conduct Company business only," and "[o]nly people appropriately authorized, for company purposes, may use the Internet[.]" Susan M. Heathfield, *Company Internet and Email Policy Sample*, (Nov. 22, 2019), http://humanresources.about.com/od/policiesandsamples1/a/email_policy.htm.

[13] *See, e.g.*, *Employee Handbook Template*, hrVillage http://www.hrvillage.com/downloads/Employee-Handbook-Template.pdf ("The policies stated in this handbook are subject to change at any time at the sole discretion of the Company."); *Employment Policies and Procedures Manual*, Dartmouth College, http://www.dartmouth.edu/~hrs/policy ("The policies are intended as guidelines only, and they may be modified, supplemented, or revoked at any time at the College's discretion.").

criminally punishable at any given time. It would enable "private parties to manipulate their computer-use and personnel policies" so as to turn employer-employee or company-consumer relationships—relationships traditionally governed by tort and contract law—"into ones policed by the criminal law." *Id*. This would grant employers and website operators the power to unilaterally "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id*.

Corporations already knowingly wield this power in jurisdictions that have broadly interpreted the CFAA. As the Seventh Circuit noted in one case, an employee of a corporate plaintiff advised in an internal email that the company "could make screen-scraping or web-harvesting illegal with a 'simple disclaimer that states the information can't be scraped from the image.'" *Fidlar Techs. v. LPS Real Estate Data Sols., Inc.*, 810 F.3d 1075, 1082 (7th Cir. 2016).

The City's Section 502 interpretation is far worse than the efforts to elevate terms of service violations into civil and criminal liability under the CFAA. Here the City argues members of the public should have known—when they learned of a publicly available file-sharing "outbox" that appeared to be a part of the City's website—that the City had nonetheless *not* granted them access to any materials within the file sharing service.

The City proposes that journalists perusing a website used to disclose public records must guess whether particular documents are

intended for them or not, intuit the City's intentions in posting those documents, and then politely look the other way—or be criminally liable. This scheme results in unclear, subjective, and after-the-fact determinations based on the whims of public officials. Effectively, the public would have to engage in mind reading to know whether officials approve of their access or subsequent use of the documents from the City's website.

City officials' unchecked discretion to decide when people used public records without permission would also create incurable notice problems. This case is even further removed from those described above that premised CFAA liability on vague or easily changed computer use policies. Here, Section 502's liability turns on government officials' individual determinations that a particular use of information from a publicly available website was without permission. Under this theory, an Internet user accessing public records via the City's publicly available website does not know when that access is "without permission," short of obtaining explicit, affirmative consent from the City prior to accessing those files.

When Internet users access public records via publicly available links, they assume the opposite: that the City has permitted access to the records. Indeed, absent technical measures or other clear and explicit notice from the City that access to documents on its publicly available website is without permission, there is almost no way any person would know

whether they had violated Section 502.

By subjecting an untold number of Internet users to potential prosecution, the City's expansive interpretation of Section 502 enables prosecutors to pick and choose which types of violations "are so morally reprehensible that they should be punished as crimes[.]" *See United States v. Kozminski*, 487 U.S. 931, 949 (1988). By giving that inherently legislative power to prosecutors, the City has "invit[ed] discriminatory and arbitrary enforcement," including of Appellants here. *See Nosal I*, 676 F.3d at 862. The Constitution, however, "does not leave us at the mercy of noblesse oblige" by the government. *United States v. Stevens*, 559 U.S. 460, 480 (2010). Rather, it requires that criminal statutes be clear.

CONCLUSION

For these reasons, this Court should reverse the superior court's entry of the preliminary injunction.

Dated: January 4, 2021

By: /s/ *Mark Rumold*
Mark Rumold

Andrew Crocker
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
T: (415) 436-9333
F: (415) 436-9993
mark@eff.org

Peter Bibring (SBN 223981)
Mohammad Tajsar (SBN 280152)
ACLU FOUNDATION OF
SOUTHERN CALIFORNIA
1313 West Eighth Street
Los Angeles, California 90017
T: (213) 977-5295
F: (213) 915-5297

Brett Max Kaufman
Esha Bhandari
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Fl.
New York, NY 10004
T: (212) 549-2500
F: (212) 549-2652

Jennifer Stisa Granick (SBN 168423)
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
T: (415) 343-0758
F: (415) 255-1478

Counsel for Amici Curiae

CERTIFICATE OF WORD COUNT

I certify pursuant to California Rules of Court 8.204 and 8.504(d) that this BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA IN SUPPORT OF APPELLANTS is proportionally spaced, has a typeface of 13 points or more, contains 6,344 words, excluding the cover, the tables, the signature block, verification, and this certificate, which is less than the total number of words permitted by the Rules of Court. Counsel relies on the word count of the Microsoft Word word-processing program used to prepare this brief.

Dated: January 4, 2021

/s/ Mark Rumold
Mark Rumold

ELECTRONIC FRONTIER FOUNDATION

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

The undersigned declares,

I am over the age of 18 years and not a party to the within action. My business address is 815 Eddy Street, San Francisco, California 94109.

On January 4, 2021, I caused to be served copies of the foregoing documents described as:

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA IN SUPPORT OF APPELLANTS

on the attached Service List

X BY TRUEFILING: I caused to be electronically filed the foregoing document with the court using the court's e-filing system. The following parties and/or counsel of record are designated for electronic service in this matter on the TrueFiling website.

X BY FIRST CLASS MAIL: I caused to be placed the envelope for collection and mailing following our ordinary business practices. I am readily familiar with this firm's practice for collecting and processing correspondence for mailing. On the same day that correspondence is placed for collection and mailing, it is deposited in the ordinary course of business with the United States Postal Service, in a sealed envelope with postage fully prepaid

Executed on January 4, 2021 at Phoenix, Arizona..

By: */s/ Mark Rumold*
Mark Rumold

SERVICE LIST

Kimberley Hall Barlow Jones & Mayer 3777 North Harbor Blvd. Fullerton, CA 92835 khb@jones-mayer.com *Attorneys for Plaintiff CITY OF FULLERTON*	*Via E-File Service*
Kelly A. Aviles Law Offices of Kelly A. Aviles 1502 Foothill Blvd., Ste. 103-140 La Verne, CA 91750 kaviles@opengovlaw.com *Attorneys for Defendants/Appellants FRIENDS FOR FULLERTON'S FUTURE, JOSHUA FERGUSON, and DAVID CURLEE*	*Via E-File Service*
Hon. James L. Crandall Dept. 33 Orange County Superior Court 700 Civic Center Drive West Santa Ana, CA 92701	*Via First Class Mail*