1st. Civ. No. G058506

IN THE COURT OF APPEAL FOR THE STATE OF CALIFORNIA
FOURTH APPELLATE DISTRICT, DIVISION 3

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

Petitioners,

v.

SUPERIOR COURT OF ORANGE COUNTY,

Respondent.

CITY OF FULLERTON,

Real Party in Interest.

Appeal from the Superior Court for the County of Orange
The Honorable Thomas Delaney
Case No. 30-2019-01107063

AMICUS CURIAE BRIEF OF THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PETITIONERS

---

*Mark Rumold (SBN 279060)
**Counsel of Record*
Andrew Crocker (SBN 291596)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: 415-436-9333
mark@eff.org
andrew@eff.org

Counsel for Amicus Curiae Electronic Frontier Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

The City of Fullerton stored documents online that any Internet user in the world could access. Unsurprisingly, Internet users found those documents, and they were then re-published—this time, with commentary and analysis of the documents themselves.

This Court should reject the City's misguided attempt to assign liability to others for its own failure to limit access to that information. Any obligation to protect allegedly confidential information contained in those documents resided with the City, not the journalists who analyzed and published them.

Although this case presents several issues central to EFF's interest in promoting free expression online,[1] this brief focuses on only one: the interpretation and application of laws written to prohibit computer hacking—here, the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and California's Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502.

---

[1] For example, the Superior Court's order imposed an unconstitutional prior restraint on Petitioners—prohibiting them from publishing information about a matter of public concern. As Petitioners and amicus Reporters Committee for Freedom of the Press have explained, First Amendment precedent prohibiting prior restraints is robust. *See, e.g.*, *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976). The prior restraint must be set aside.

Several key terms in these statutes are notoriously vague and, if misconstrued, risk creating civil and criminal liability for a wide swath of common and innocuous online behavior. For this reason, EFF urges the Court to exercise caution when interpreting and applying these statutes to the conduct at issue here.

Indeed, based on our understanding of the facts, liability under the CFAA and CDAFA simply *cannot* attach.

I. The full contents of the City's Dropbox account were available to any Internet user in the world.

The City alleges Petitioners violated the CFAA and CDAFA by accessing a City Dropbox account that had no password protection or any other technical access barrier—in other words, the account was *publicly accessible to any person in the world with an Internet connection*. *See* Petition for Extraordinary Writ of Mandate, Prohibition, and/or Other Appropriate Relief, ¶ 19; Declaration of John Bambenek in Support of Opposition to OSC re: Preliminary Injunction ("Bambenek Decl."), ¶ 19, *filed in City of Fullerton v. Friends for Fullerton's Future, et al*., 2019-01107063.

Critically, any Internet user in the world could visit the City's URL—www.cityoffullerton.com/outbox—and: (1) access the entire

contents of the City's Dropbox account, and (2) download any file stored in the account. Bambenek Decl., ¶ 20.[2]

II. Accessing data publicly available to any Internet user cannot create liability under CFAA or CDAFA.

The CFAA creates liability for intentionally accessing a protected computer to obtain information "without authorization" or for "exceed[ing] authorized access." 18 U.S.C. § 1030(a)(2)(C). Similarly, liability exists under CDAFA for taking, copying, or making use of data from a computer "without permission." Cal. Penal Code § 502(c)(2).

Thus, whether a defendant's use or access to a computer was permitted or authorized is central to liability under both statutes. As the Ninth Circuit has explained, "despite differences in wording, the analysis under both statutes is similar." *Power Ventures*, 844 F.3d at 1069; *see also United States v. Nosal*, 844 F.3d 1024, 1028 (9th Cir. 2016) (holding

---

[2] It appears some files stored in the account required a password to *unzip* the file. However, no password was required to download the zipped file from the Dropbox account to a user's computer.

The process of unzipping a file does not implicate the CFAA because that statute does not reach subsequent use of data that was accessed with authorization. *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) ("*Nosal I*"). Meanwhile, although the CDAFA does encompass use of data "without permission," the burden is on the plaintiff to demonstrate that use was unpermitted. The City has not demonstrated that the Petitioners unzipped any files without permission. Indeed, the City provided them the password to do so. *See Facebook v. Power Ventures*, 844 F.3d 1058, 1069 (9th Cir. 2016) (CDAFA is not violated where defendant has "implied authorization" to access and use data).

"'without authorization' is an unambiguous, non-technical term" that means "without permission"); Black's Law Dictionary (10th ed. 2014) (defining "authorization" as "[o]fficial permission").

Where information is publicly available to any Internet user—like the City's Dropbox account was here—courts recognize that *everyone* using the Internet is "authorized" to access the data. *See, e.g., hiQ Labs, Inc. v. LinkedIn Corporation*, 938 F.3d 985, 1000 (9th Cir. 2019) (acknowledging that "where access is open to the general public, the CFAA 'without authorization' concept is inapplicable"); *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 information 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*, 938 F.3d at 1002.

The same is true under CDAFA: a party only acts "without permission" when it circumvents technical barriers to a user's access. *See Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1053 (N.D. Cal. 2018) (acting "without permission" requires "circumvention of technical or code-

based barriers in place to restrict or bar a user's access"); *In re Facebook Privacy Litigation*, 791 F. Supp. 2d 705, 716 (N.D. Cal. 2011) (same).

The City could have (and, indeed, likely *should 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 the account as a whole, or by more granularly managing access to particular folders within the account. Indeed, Dropbox offers all these capabilities. *See* Bambenek Decl. ¶¶ 13-18. This would have allowed the City to let authorized users in and keep unwanted individuals out.

But—whether intentionally or inadvertently—the City did not. It left its account wholly available to any Internet user and even affirmatively shared the account with members of the public. Under these circumstances, Petitioners have not violated the CFAA or CDAFA.

III. The legislative purpose of the CFAA and CDAFA and sound policy preclude liability in this case.

Courts recognize the need to interpret the CFAA narrowly, both in keeping with the statute's legislative purpose and to avoid criminalizing a wide variety of common online behaviors. CDAFA should be interpreted similarly.

The CFAA was enacted to prevent computer hacking. *hiQ*, 938 F.3d at 1000-01 (reviewing legislative history). The conduct prohibited under the statute is thus "analogous to that of 'breaking and entering.'" *Id*. at 1001.

In contrast, the CFAA is *not* a "misappropriation statute," designed to criminalize disfavored or unauthorized use of information obtained from a computer. *Nosal I*, 676 F.3d at 863. The statute likewise does not create liability for merely violating a website's terms of use. *Id*. at 862; *Power Ventures, Inc.*, 844 F.3d at 1067 ("[A] violation of the terms of use of a website—without more—cannot establish liability under the CFAA.").

As the Ninth Circuit explained in *hiQ*:

> The legislative history of [the CFAA] thus makes clear that the prohibition on unauthorized access is properly understood to apply only to private information—information delineated as private through use of a permission requirement of some sort.

938 F.3d at 1001.[3] This legislative purpose, in turn, bolsters the conclusion that authorization is only required for "password-protected sites or sites that otherwise prevent the general public" from accessing information—unlike the City Dropbox account here. *Id*.

The same is true of the CDAFA. In *Chrisman v. City of Los Angeles*, 155 Cal. App. 4th 29 (2007), the Court of Appeal recognized that a primary legislative purpose of CDAFA is to deter computer hackers—those

[3] This interpretation, too, is consistent with the open-access norms of the Internet more generally. *See* Orin Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1161 (2016). The City's technical expert's suggestion that an "unlocked door is not a defense to burglary," Decl. of Matthew Strebe ¶ 18—aside from being a legal conclusion well beyond his technical expertise—wholly ignores these important and well established norms. *See hiQ*, 938 F.3d at 1001-2.

"outsiders who *break into a computer system* to obtain or alter the information contained there." 155 Cal. App. 4th at 34 (quoting *People v. Gentry*, 234 Cal. App. 3d 131 (1991)) (emphasis added). The *Chrisman* court contrasted that type of "hacking," which is prohibited by CDAFA, with using a computer in an intended manner, but accessing data for an illicit or unapproved purpose—conduct beyond the statute's reach. 155 Cal. App. 4th at 35.[4] Other courts, too, have limited the scope of some of CDAFA's broadest terms. *See Ticketmaster, LLC v. Prestige Entertainment West, Inc.*, 315 F. Supp. 3d 1147, 1175 n.5 (C.D. Cal. 2018) (imposing narrowing construction on "or otherwise uses" data).

Cabining these statutes to their intended purpose—prohibiting computer hacking—is critical: anything less risks criminalizing a wide swath of everyday online activity. Under expansive interpretations of these statutes, an employer's computer-use policy or the obscure fine print of a website's terms-of-use could operate to define state and federal crimes. *Nosal I*, 676 F.3d at 860-62. And, just as in *Nosal*, if this Court were to adopt the City's proposed interpretation of CDAFA and the CFAA,

[4] Other Courts of Appeal have interpreted the statute differently. *See, e.g.*, *Gilbert v. Sunnyvale*, 130 Cal. App. 4th 1264, 1281 (2005). In EFF's view, however, the *Chrisman* Court's interpretation is most faithful to CDAFA's legislative purpose and sound public policy.

"millions of unsuspecting individuals" could "find that they are engaging in criminal conduct." *Id*. at 859.

CONCLUSION

Neither the CFAA nor the CDAFA create a "sweeping Internet-policing mandate." *Id*. at 858. But that is precisely how the City attempts to use these laws here: to create liability for the access and use of data that the City, itself, left open to the public.

EFF urges the Court to reject the City's attempt to expand these statutes to govern the conduct described here.

Respectfully submitted,

Dated: November 21, 2019

/s/ *Mark Rumold*
Mark Rumold

Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
mark@eff.org
andrew@eff.org

Counsel for Amicus Curiae Electronic Frontier Foundation

CERTIFICATE OF WORD COUNT

I certify pursuant to California Rules of Court 8.204 and 8.504(d) that this Amicus Brief of Electronic Frontier Foundation, is proportionally spaced, has a typeface of 13 points or more, contains 1,694 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: November 21, 2019

/s/ Mark Rumold
Mark Rumold

ELECTRONIC FRONTIER FOUNDATION

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

STATE OF CALIFORNIA, COUNTY OF SAN FRANCISCO

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 November 21, 2019, I caused to be served copies of the foregoing document entitled:

AMICUS CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PETITIONERS

on the attached Service List

X BY ELECTRONIC TRANMISSION VIA TRUEFILING: I caused a copy of the foregoing documents to be sent via TrueFiling to the persons at the e-mail addresses listed in the Service List. The following parties and/or counsel of record are designated for electronic service in this matter on the TrueFiling website. I did not receive, within a reasonable time after the transmission, any electronic message or other indication that the transmission was unsuccessful.

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 November 21, 2019 at Phoenix, Arizona.

/s/ *Mark Rumold*
Mark Rumold

SERVICE LIST

Kelly A. Aviles
Law Offices of Kelly Aviles
1502 Foothill Boulevard
Suite 103-140
La Verne, CA 91750
kaviles@opengovlaw.com

Via E-File Service

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

Via E-File Service

Counsel for Plaintiff and Real Party in Interest City of Fullerton

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

Via First Class Mail