No. 17-16783

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

HIQ LABS, INC.,

Plaintiff-Appellee,

v.

LINKEDIN CORPORATION,

Defendant-Appellant.

On Appeal from the United States District Court for the
Northern District of California
Case No. 3:17-cv-03301-EMC (The Honorable Edward M. Chen)

[PROPOSED] BRIEF OF AMICI CURIAE THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS AND 30 NEWS MEDIA ORGANIZATIONS IN SUPPORT OF NEITHER PARTY

[Caption continued on next page]

Katie Townsend
Counsel of Record for Amici Curiae
Bruce D. Brown*
Gabe Rottman*
Grayson Clary*
Mailyn Fidler*
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th St. NW, Suite 1020
Washington, D.C. 20005
Telephone: (202) 795-9300
Facsimile: (202) 795-9310
**Of counsel*

CORPORATE DISCLOSURE STATEMENTS

The Reporters Committee for Freedom of the Press is an unincorporated association of reporters and editors with no parent corporation and no stock.

The Associated Press is a global news agency organized as a mutual news cooperative under the New York Not-For-Profit Corporation law. It is not publicly traded.

The Atlantic Monthly Group LLC is a privately held media company, owned by Emerson Collective and Atlantic Media, Inc. No publicly held corporation owns 10% or more of its stock.

Boston Globe Media Partners, LLC, is a privately held company. No publicly held corporation owns 10% or more of its stock.

BuzzFeed Inc. is a privately owned company, and National Broadcasting Company (NBC) owns 10% or more of its stock.

Californians Aware is a nonprofit organization with no parent corporation and no stock.

The Center for Investigative Reporting (d/b/a Reveal) is a California non-profit public benefit corporation that is tax-exempt under section 501(c)(3) of the Internal Revenue Code. It has no statutory members and no stock.

The Center for Public Integrity is a nonprofit organization with no parent corporation and no stock.

Dow Jones & Company, Inc. ("Dow Jones") is an indirect subsidiary of News Corporation, a publicly held company. Ruby Newco, LLC, an indirect subsidiary of News Corporation and a non-publicly held company, is the direct parent of Dow Jones. News Preferred Holdings, Inc., a subsidiary of News Corporation, is the direct parent of Ruby Newco, LLC. No publicly traded corporation currently owns ten percent or more of the stock of Dow Jones.

First Amendment Coalition is a nonprofit organization with no parent company. It issues no stock and does not own any of the party's or amicus' stock.

Freedom of the Press Foundation does not have a parent corporation, and no publicly held corporation owns 10% or more of the stock of the organization.

Gannett Co., Inc. is a publicly traded company and has no affiliates or subsidiaries that are publicly owned. BlackRock, Inc. and the Vanguard Group, Inc. each own ten percent or more of the stock of Gannett Co., Inc.

Hearst Corporation is privately held and no publicly held corporation owns 10% or more of Hearst Corporation.

The International Documentary Association is an not-for-profit organization with no parent corporation and no stock.

The Investigative Reporting Workshop is a privately funded, nonprofit news organization based at the American University School of Communication in Washington. It issues no stock.

Los Angeles Times Communications LLC is wholly owned by NantMedia Holdings, LLC.

The Media Institute is a 501(c)(3) non-stock corporation with no parent corporation.

The National Freedom of Information Coalition is a nonprofit organization that has not issued any shares or debt securities to the public, and has no parent companies, subsidiaries, or affiliates that have issued any shares or debt securities to the public.

National Press Photographers Association is a 501(c)(6) nonprofit organization with no parent company. It issues no stock and does not own any of the party's or amicus' stock.

National Public Radio, Inc. is a privately supported, not-for-profit membership organization that has no parent company and issues no stock.

The New York Times Company is a publicly traded company and has no affiliates or subsidiaries that are publicly owned. No publicly held company owns 10% or more of its stock.

The News Leaders Association has no parent corporation and does not issue any stock.

Newsday LLC is a Delaware limited liability company whose members are Tillandsia Media Holdings LLC and Newsday Holdings LLC. Newsday Holdings LLC is an indirect subsidiary of Cablevision Systems Corporation. Cablevision Systems Corporation is (a) directly owned by Altice USA, Inc., a Delaware corporation which is publicly traded on the New York Stock Exchange and (b) indirectly owned by Altice N.V., a Netherlands public company.

Online News Association is a not-for-profit organization. It has no parent corporation, and no publicly traded corporation owns 10% or more of its stock.

No publicly held corporations own any stock in the Philadelphia Inquirer, PBC, or its parent company, the non-profit Lenfest Institute for Journalism, LLC.

Radio Television Digital News Association is a nonprofit organization that has no parent company and issues no stock.

The Seattle Times Company: The McClatchy Company, LLC owns 49.5% of the voting common stock and 70.6% of the nonvoting common stock of The Seattle Times Company.

The Society of Environmental Journalists is a 501(c)(3) non-profit educational organization. It has no parent corporation and issues no stock.

Society of Professional Journalists is a non-stock corporation with no parent company.

The Tully Center for Free Speech is a subsidiary of Syracuse University.

WNET is a not-for-profit organization, supported by private and public funds, that has no parent company and issues no stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF IDENTITY AND INTEREST OF AMICI CURIAE

Amici curiae are the Reporters Committee for Freedom of the Press (the "Reporters Committee") and The Associated Press, The Atlantic Monthly Group LLC, Boston Globe Media Partners, LLC, BuzzFeed, Californians Aware, The Center for Investigative Reporting (d/b/a Reveal), The Center for Public Integrity, Dow Jones & Company, Inc., First Amendment Coalition, Freedom of the Press Foundation, Gannett Co., Inc., Hearst Corporation, International Documentary Association, Investigative Reporting Workshop at American University, Los Angeles Times Communications LLC, The Media Institute, National Freedom of Information Coalition, National Press Photographers Association, National Public Radio, Inc., The New York Times Company, The News Leaders Association, Newsday LLC, Online News Association, The Philadelphia Inquirer, Radio Television Digital News Association, The Seattle Times Company, Society of Environmental Journalists, Society of Professional Journalists, Tully Center for Free Speech, and WNET (collectively, "amici"). A supplemental statement of identity and interest is included as Appendix A to the motion filed herewith.

SOURCE OF AUTHORITY TO FILE

Amici respectfully request leave to file by the motion filed herewith. *See* Fed. R. App. P. 27; Cir. R. 29-3. Plaintiff-Appellee and Defendant-Appellant have represented that they consent to filing of this brief. *Cf.* Fed. R. App. P. 29(a)(2).

FED. R. APP. P. 29(a)(4)(E) STATEMENT

Amici declare that:

1. no party's counsel authored the brief in whole or in part;
2. no party or party's counsel contributed money intended to fund preparing or submitting the brief; and
3. no person, other than amici, their members or their counsel, contributed money intended to fund preparing or submitting the brief.

INTRODUCTION

As this Court has consistently recognized, the Computer Fraud and Abuse Act (CFAA) prohibits "hacking"; it is not a "sweeping Internet-policing mandate." *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1003 (9th Cir. 2019), *vacated and remanded*, No. 19-1116, 2021 WL 2405144 (U.S. June 14, 2021) (citation omitted). In *Van Buren v. United States*, 141 S. Ct. 1648 (2021), the Supreme Court endorsed that view, drawing a clear line between the "hackers" the CFAA targets, *id.* at 1658, and the "millions of otherwise law-abiding citizens"—including those engaged in "journalism activity"—who cannot be punished for offending a site owner's private preferences, *id.* at 1661. That distinction provides essential protection for reporters exercising the First Amendment right to gather the news. This Court should reject Defendant-Appellant's invitation to unwind it.[1]

Website operators frequently expose newsworthy information about themselves to the public, either without intending to or hoping no one will notice. Just as often, journalists and researchers use techniques like scraping to surface that information in the public interest. And too often, platforms react by ordering that reporters not record what the platforms themselves have chosen to publish.

---

[1] Because amici take no position on other, potentially dispositive issues presented in the underlying appeal, amici proffer this brief in support of neither party.

See, e.g., Victoria Baranetsky, *Data Journalism and the Law*, Tow Ctr. for Digital Journalism (Sept. 9, 2018), https://perma.cc/2D5C-Q2GB. *Van Buren*, though, makes clear a party cannot purport to bar access with one hand while displaying the same information to the world with the other. What the CFAA requires is "a gates-up-or-down inquiry." *Van Buren*, 141 S. Ct. at 1658. Plainly no gate protects pages that are "accessible to the general public," *hiQ*, 938 F.3d at 1001, and plainly the press could not be punished for observing what any other member of the public may, *cf. Index Newspapers LLC v. U.S. Marshals Serv.*, 977 F.3d 817, 830 (9th Cir. 2020) (noting that the right of the press to observe a given place or process is "at least coextensive with the right enjoyed by the public at large").

Were it otherwise—if a website owner could forbid journalists from observing what any eye can see, like a shop owner policing which pedestrians can look at a window display—the CFAA would raise grave constitutional questions under the First Amendment and the Due Process Clause. *Van Buren* did not have occasion to address those concerns, 141 S. Ct. at 1661, but they underline the importance of giving *Van Buren*'s distinction between hacking and conventional internet use full effect. Because Defendant-Appellant's interpretation would muddy that line, threatening ordinary online "journalism activity" with civil liability and criminal sanctions, *id.*, amici respectfully urge this Court to reject it.

ARGUMENT

I. *Van Buren* confirmed the CFAA does not bar "journalism activity."

Van Buren's core holding is clear: Whether a party is accused of accessing a computer "without authorization" or of "exceed[ing] authorized access," 18 U.S.C. § 1030(a)(2), "liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system," *Van Buren*, 141 S. Ct. at 1658–59. That test excludes "circumstance-based access restrictions," like an internet user's "agreement to follow specified terms of service" that limit access to certain manners or purposes. *Id.* at 1661; *see also id.* at 1660 n.11 (rejecting the dissent's suggestion that the statute embraces "'time and manner' restrictions" as well as "purpose-based ones"). Otherwise, the CFAA would operate to criminalize a sweeping range of trivial, innocuous, or forthrightly publicly beneficial conduct, including "journalism activity" and "online civil-rights testing and research." *Id.*[2]

[2] As this Court has noted, the CFAA is a dual civil-criminal statute, and courts must "interpret the statute consistently"—applying the rule of lenity, for instance—even if a case involves only civil liability. *hiQ*, 938 F.3d at 1003 (quoting *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004)). Accordingly, as chilling as such liability can be where press rights are at risk, *see Sessions v. Dimaya*, 138 S. Ct. 1204, 1228–29 (2018) (Gorsuch, J., concurring), amici also refer to the criminal consequences of Defendant-Appellant's interpretation of the CFAA in this brief.

Take, for instance, the role of scraping—the automated process of pulling large amounts of information from websites—in data journalism. Scraping typically does not expose any information beyond what could be found through manual operation of the website by a user with ordinary privileges. Instead, its advantage is that it "speeds up the tedious job of manually copying and pasting data into a spreadsheet, making large-scale data collection possible." Jacquellena Carrero, Note, *Access Granted: A First Amendment Theory of Reform of the CFAA Access Provision*, 120 Colum. L. Rev. 131, 137 (2020); *cf. hiQ*, 938 F.3d at 991 n.5 (noting that LinkedIn's terms of service do not distinguish between "manual" copying and the use of "any other technology" to gather the same information).

The results, though, after comprehensive data collection and analysis, can reveal much more than any one user visiting the website would have noticed. And reporting relying on these techniques has been used to expose, among other things, unlawful private discrimination and important public failings. *See, e.g.*, Noa Yachot, *Your Favorite Website Might Be Discriminating Against You*, ACLU (June 29, 2016, 9:45 AM), https://perma.cc/6W67-68J4; 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. Unsurprisingly, subjects of that sort of reporting would like a license to quash it.

Many websites now routinely purport to forbid scraping—or otherwise using the information they host for journalistic or research purposes—in their terms of service, even as the information remains on public display. *See* Carrero, *supra*, at 134. If violating those private preferences were the measure of CFAA liability, it would be up to the subject of an exposé to decide whether to criminalize routine investigative reporting techniques in any particular case. As discussed *infra* Part III, while *Van Buren* did not reach the question, a reading of the law that permitted that result would raise serious questions about the CFAA's constitutional validity.

But *Van Buren* by its own terms shields data journalism by excluding circumstantial access restrictions from the scope of the statute. *See* 141 S. Ct. at 1661; *id.* at 1659 & n.10 (explaining that neither the "without authorization" nor the "exceeds authorized access" prong incorporates such restrictions). Only when a gate bars access to a particular individual entirely can liability attach. *See id.* at 1658; *id.* at 1663 (Thomas, J., dissenting) (characterizing the majority's "gate" rule as one under which entitlement "to obtain information in at least *one* circumstance" defeats liability). And because data journalism techniques like scraping typically rely only on the same access any user would enjoy—the access a journalist could lawfully exercise in their capacity as a member of "the general public," *hiQ*, 938 F.3d at 1001—the CFAA cannot be wielded to punish them.

II. Defendant-Appellant's reading of the CFAA would prohibit routine journalism and undermine the guardrails established in *Van Buren*.

Defendant-Appellant nevertheless maintains that *Van Buren* does not govern when a website takes the further step of blocking an IP address associated with a user who violated its terms, or otherwise tells the user to stop. *See* Defendant-Appellant's Br. 7. If that were so, the limit announced in *Van Buren* would be of little use, and the parade of horribles that "underscore[d] the implausibility" of the reading the Supreme Court rejected would spring back to life. 141 S. Ct. at 1661.

After all, a cease-and-desist letter simply restates the same terms-of-service violation that *Van Buren* held cannot support charges under the statute. For just that reason, this Court has observed that letting a site sue on a "boilerplate" notice "follow[ing] a violation of a website's terms of use" would be in considerable "tension" with the principle that the terms themselves cannot be the basis for CFAA liability. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 n.1 (9th Cir. 2016). And 'tension' puts it mildly: In fact, the expedient of copying a provision from the terms onto letterhead would effectively eliminate the guardrails the Supreme Court believed it was establishing in *Van Buren*. "An interpretation that stakes so much on a fine distinction controlled by the drafting practices of private parties is hard to sell as the most plausible," *Van Buren*, 141 S. Ct. at 1662, and such an approach would provide no safe harbor at all for newsgathering rights.

Van Buren does not, in fact, permit that approach. As to the IP blocks, such measures are not a "gate" because they do not bar a user from accessing the site entirely, only in a particular "manner": by using that IP address rather than a different one. *Van Buren*, 141 S. Ct. at 1659 n.10. But "IP blocking cannot keep anyone out" if a page is otherwise published to the public, because changes to a user's IP address occur routinely in the course of ordinary internet use. Orin S. Kerr, Essay, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1169 (2016). As to the cease-and-desist letter, Defendant-Appellant relies heavily on footnote 8 of *Van Buren*, which reserved the issue whether the existence of a gate "turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies." 141 S. Ct. at 1659 n.8. But that footnote can hardly be read as a retreat from the principle that terms-of-service violations cannot support liability, *id.* at 1661, because requiring a simple letter would cure none of the harms associated with punishing breaches of the terms themselves.[3]

[3] Footnote 8 means what it says: Some of the rules that distinguish insiders from outsiders may be norm-based rather than code-based. For instance, code alone cannot explain why a journalist is an insider when entering her own email password and a hacker when guessing a stranger's—the act of typing the password is technologically identical in each case. *Cf.* 18 U.S.C. § 1030(a)(6) (prohibiting password trafficking). But the boundaries of that principle are irrelevant here. Norms may clarify when entering a password is "hacking," *Van Buren*, 141 S. Ct. at 1660, but visiting a URL that was published to the open internet simply never is.

It would do nothing, for instance, to narrow the "breathtaking amount of commonplace computer activity" that would be punishable *after* taking the de minimis effort of sending a letter. *Id.* It would do nothing to protect "journalism activity" or "online civil-rights testing and research," *id.*, since platforms would be happy to take the extra step of sending an email if it means avoiding critical press coverage. And while Defendant-Appellant represents on behalf of all websites that letters will not be sent "indiscriminately," Defendant-Appellant's Br. 17, it identifies no legal limit on a site's ability to do so. "A court should not uphold a highly problematic interpretation of a statute merely because" a party "promises to use it responsibly." *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015). Such a rule would "inject arbitrariness into the assessment of criminal liability," *Van Buren*, 141 S. Ct. at 1662, and have as severe a chilling effect on reporting as if an underlying restriction on journalistic purposes were directly enforceable. No one will launch an investigation in the first instance if it can be so trivially killed.

Most importantly, for purposes of *Van Buren*, such a letter does nothing to draw an intelligible line between "outside hackers" and authorized insiders if the information at issue remains published to the open internet. 141 S. Ct. at 1658. Demanding that a user not look at that public content is akin to "publishing a newspaper but then forbidding someone to read it," or ordering a newspaper to

stop taking notice of the existence of a press release. Kerr, *supra*, at 1169. The letter does not change the reality that Defendant-Appellant has supplied and continues to supply Plaintiff-Appellee with the authorization that ensures Plaintiff-Appellee "can . . . access" the website: the URL. *Van Buren*, 141 S. Ct. at 1658. At base, like the IP block, such a letter is merely a restatement of the underlying circumstance-based restriction, not a true all-or-nothing gate.[4] Under *Van Buren*, the CFAA cannot be used to enforce it—not without reintroducing the chilling "arbitrariness" that the Supreme Court's decision condemned. 141 S. Ct. at 1662.

III. Defendant-Appellant's reading of the CFAA would raise serious questions about the statute's constitutionality that *Van Buren* reserved.

Defendant-Appellant's reading of the CFAA would also call into question the statute's constitutionality. *Van Buren* reserved that issue, but constitutional avoidance should and must inform this Court's decision if it considers Defendant-Appellant's interpretation of the CFAA plausible. *See Clark v. Martinez*, 543 U.S. 371, 380–81 (2005) (when one of two "plausible statutory constructions" would raise "constitutional problems, the other should prevail"). Indeed, while this Court

[4] While Defendant-Appellant claims that this Court concluded otherwise in *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), *Power Ventures* stressed that that case did "*not* involve non-compliance with terms and conditions of service," *id.* at 1069, and did not decide whether a letter alleging only such non-compliance could provide a predicate for CFAA liability, *id.* at 1067 n.3.

need not resolve the underlying constitutional question itself, avoidance should cut against Defendant-Appellant's reading if it so much as "presents a significant risk" of infringing a constitutional right. *NLRB v. Catholic Bishop of Chi.*, 440 U.S. 490, 502 (1979). On due process and First Amendment grounds, it plainly does.

A. A broad interpretation of the CFAA would violate the vagueness doctrine.

Defendant-Appellant's interpretation squarely implicates the separation-of-powers and due process concerns that underpin the vagueness doctrine. Its reading makes "each webmaster into [its] own legislature," *Sandvig v. Barr*, 451 F. Supp. 3d 73, 88 (D.D.C. 2020), delegating the task of defining criminal conduct to private parties, *United States v. Davis*, 139 S. Ct. 2319, 2325 (2019) (noting that "hand[ing] responsibility for defining crimes" to an actor other than the legislature "erod[es] the people's ability to oversee the creation of the laws"); *see* Peter W. Low & Joel S. Johnson, *Changing the Vocabulary of the Vagueness Doctrine*, 101 Va. L. Rev. 2051, 2053 (2015) (identifying an "antidelegation" principle in the Court's vagueness decisions). This view would incorporate widely varying computer-use policies and terms of service into the federal criminal code, placing the power to determine federal criminal law in non-legislative hands. *United States v. Kozminski*, 487 U.S. 931, 949–950, 952 (1988) (critiquing "delegat[ing]" the "inherently legislative task of determining what type of . . . activities are so

morally reprehensible that they should be punished as crimes"). Moreover, because parties can change their terms of service at any time and for any reason, behavior Congress never had in view when it enacted the CFAA could be made criminal without any action by the public's representatives. Requiring that a site send a letter explaining *what* it criminalized on a whim does not fix the problem.

Defendant-Appellant's view of the statute would also fail to provide sufficient notice of criminal conduct, turning the CFAA into an "unworkable and standardless" law. *Sandvig*, 451 F. Supp. 3d at 88. Such a law implicates the vagueness doctrine's due process component, including by inviting arbitrary enforcement. *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972); *see also Davis*, 139 S. Ct. at 2326; Low & Johnson, *supra*, at 2053; Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 Harv. L. Rev. 751, 768–771 (2013). The fair notice problem becomes even more troubling because websites' terms of service often use broad and indefinite language to forbid a wide range of ordinary activity, such as the blanket prohibition on posting "bad stuff" that was at one point included in YouTube's terms. *See* David A. Puckett, *Terms of Service and the Computer Fraud and Abuse Act: A Trap for the Unwary?*, Okla. J. L. & Tech., Jan. 2011, at 1, 20. Defendant-Appellant claims a letter is notice enough, Defendant-Appellant's Br. 16, but even

on its view not all such letters can support liability, *see id.* at 17. Apparently the recipient must guess which are the kind that criminalize and which are not.

Cease-and-desist notices and IP blocks also do not reduce the risk that relying on terms of service to define offenses under the CFAA "invites arbitrary enforcement." *Johnson v. United States*, 135 S. Ct. 2551, 2556 (2015). That arbitrariness poses a particular danger for the press, who risk being singled out by, say, a government official who perceives the substance of a given investigation as critical of the state, or a private party who would rather not have their own illegal conduct revealed. *Cf. Nieves v. Bartlett*, 139 S. Ct. 1715, 1727 (2019) (noting that special retaliation concerns are raised by offenses that, like jaywalking, are often committed but rarely charged). Defendant-Appellant's suggestion that cease-and-desists will be sent sparingly, only when a platform truly cares to criminalize, *see* Defendant-Appellant's Br. 17, drives home that its reading of the statute, if adopted, would confer too much discretion and render the CFAA too vague.

B. A broad interpretation of the CFAA would chill the exercise of First Amendment rights.

The interpretation of the CFAA urged by Defendant-Appellant would also threaten to outlaw a significant amount of journalism in the public interest. If adopted, even unsuccessful prosecutions would significantly chill the exercise of speech and press rights. *See, e.g.*, *Dombrowski v. Pfister*, 380 U.S. 479, 494

(1965). Recording what a website displays, after all, is just another way of exercising the right to record endorsed by at least seven courts of appeals, which have affirmed that individuals have a First Amendment right to gather information in places they otherwise have a right to be.[5] Scraping a public-facing website "is merely a particular use of information that plaintiffs are entitled to see," *Sandvig v. Sessions*, 315 F. Supp. 3d 1, 26–27 (D.D.C. 2018), and reliance on scraping rather than note-taking to record what appears does not change the fact that the First Amendment protects that activity, *see id.* at 16 (scraping is not "meaningfully different from . . . using the panorama function on a smartphone instead of taking a series of photos from different positions"). Interpreting the CFAA to foreclose such techniques would shut down newsgathering from otherwise public sources, dramatically altering the means by which the press reports the news—and the degree of newsworthy information ultimately provided to the public. *Van Buren* did not sanction that result, *see* 141 S. Ct. at 1661, and neither should this Court.

[5] *See Gericke v. Begin*, 753 F.3d 1, 7 (1st Cir. 2014); *Fields v. City of Philadelphia*, 862 F.3d 353, 359 (3d Cir. 2017); *Turner v. Lieutenant Driver*, 848 F.3d 678, 688–89 (5th Cir. 2017); *ACLU of Ill. v. Alvarez*, 679 F.3d 583, 595 (7th Cir. 2012); *Animal Legal Def. Fund v. Wasden*, 878 F.3d 1184, 1203 (9th Cir. 2018); *W. Watersheds Project v. Michael*, 869 F.3d 1189, 1195–97 (10th Cir. 2017); *Smith v. City of Cumming*, 212 F.3d 1332, 1333 (11th Cir. 2000).

CONCLUSION

For the foregoing reasons, amici respectfully urge the Court to reject Defendant-Appellant's interpretation of the CFAA.

Dated: July 16, 2021

Respectfully submitted,

/s/ Katie Townsend

Katie Townsend
Counsel of Record for Amici Curiae
Bruce D. Brown*
Gabe Rottman*
Grayson Clary*
Mailyn Fidler*
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th St. NW, Suite 1020
Washington, D.C. 20005
Telephone: (202) 795-9300
Facsimile: (202) 795-9310
**Of counsel*

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

9th Cir. Case Number(s): 17-16783

I am the attorney for *amici curiae* the Reporters Committee for Freedom of the Press and 30 News Media Organizations.

This brief contains 3,491 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[**X**] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:

[ ] it is a joint brief submitted by separately represented parties;
[ ] a party or parties are filing a single brief in response to multiple briefs; or
[ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature *s/ Katie Townsend* **Date** July 16, 2021