No. 25-1374

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

RYANAIR DAC,
Plaintiff-Appellant,

v.

BOOKING.COM B.V.,
Defendant-Appellee.

On Appeal from the United States District Court
for the District of Delaware
Civil Case No. 1:20-cv-01191 (Hon. William C. Bryson)

BRIEF OF AMICUS CURIAE THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS IN SUPPORT OF DEFENDANT-APPELLEE

Gabe Rottman
Counsel of Record for Amicus Curiae
Lisa Zycherman*
Grayson Clary*
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
grottman@rcfp.org

**Of counsel*

CORPORATE DISCLOSURE STATEMENT

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

TABLE OF CONTENTS

Page:

TABLE OF AUTHORITIES

Page(s):

Cases

Statutes

Other Authorities

SOURCE OF AUTHORITY TO FILE

The Reporters Committee respectfully requests leave to file by the motion filed herewith.

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

The Reporters Committee for Freedom of the Press declares 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 amicus, its members or its counsel, contributed money intended to fund preparing or submitting the brief.

STATEMENT OF IDENTITY AND INTEREST OF AMICUS CURIAE

The Reporters Committee for Freedom of the Press (the "Reporters Committee") is an unincorporated nonprofit association of reporters and editors, founded by leading journalists and media lawyers in 1970 when the nation's news media faced an unprecedented wave of government subpoenas forcing reporters to name confidential sources. Today, its attorneys provide pro bono legal representation, amicus curiae support, and other legal resources to protect First Amendment freedoms and the newsgathering rights of journalists.

The Reporters Committee frequently appears as amicus curiae to highlight the risks an overbroad interpretation of the Computer Fraud and Abuse Act (CFAA) would pose to routine "journalism activity." *Van Buren v. United States*, 593 U.S. 374, 394 (2021) (citing Br. for Reporters Comm. for Freedom of the Press et al. as Amici Curiae at 10–13 (No. 19-783), 2020 WL 3964377). Here, the District Court's conclusion that the CFAA prohibits accessing information that any member of the public could obtain with a free account, after the website owner sends a cease-and-desist letter, would jeopardize routine tools of data journalism, including scraping and the use of test accounts. The Reporters Committee submits this brief to call attention to that harm and explain that the CFAA cannot bear that reading.

SUMMARY OF THE ARGUMENT

In *Van Buren v. United States*, 593 U.S. 374 (2021), the Supreme Court made clear that the Computer Fraud and Abuse Act (CFAA) targets "hackers," *id.* at 389, not the "millions of otherwise law-abiding citizens"—including reporters engaged in routine "journalism"—who cannot be punished for offending a website operator's private preferences, *id.* at 394. That distinction provides essential protection for data journalists exercising the First Amendment right to gather the news online. But en route to judgment in this case, the District Court muddied that line, holding that the CFAA prohibits accessing information that any member of the public could access with a free account if an aggrieved site owner first takes the simple step of telling the user to stop. That reading of the Act would threaten the routine use of scraping and test accounts in investigative journalism—activity protected by the First Amendment, *see Sandvig v. Sessions*, 315 F. Supp. 3d 1, 15–17 (D.D.C. 2018)—with civil and criminal liability. This Court should reject it.

Frequently, website operators expose newsworthy information about their business practices to the public, either without intending to or hoping that no one will notice. Just as often, journalists and researchers use tools like scraping and test accounts to surface that information in the public interest—much as analog testers did before the advent of the Internet. *See Van Buren*, 593 U.S. at 394 (rejecting a reading of the CFAA that would prohibit "online civil-rights testing"

and "using a pseudonym on Facebook"). And too often, platforms react by ordering that reporters stop documenting what the platforms themselves chose to publish. *See, e.g.*, Jeff Horwitz, *Facebook Seeks Shutdown of NYU Research Project Into Political Ad Targeting*, Wall St. J. (Oct. 23, 2020), https://perma.cc/9W3Y-LC8V. *Van Buren*, though, makes clear that a party cannot purport to bar access with one hand while displaying the same data to the world with the other. Were it otherwise—if a website owner could forbid journalists from observing what any member of the public would be entitled to 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. And while *Van Buren* did not have occasion to address those concerns, *see* 593 U.S. at 393–94, they underline the importance of giving the statute's distinction between hacking and conventional Internet use full effect.

Because the District Court's interpretation of the CFAA would chill "journalism activity," *id.* at 394, including the routine use of test accounts in investigative reporting, amicus respectfully urges this Court to affirm the judgment on the alternative ground that Defendant-Appellee's conduct did not violate the CFAA.

ARGUMENT

I. The District Court's interpretation of the Computer Fraud and Abuse Act would allow private parties to criminalize routine data journalism.

Just as the "vast democratic forums of the Internet" provide today some of "the most important places . . . for the exchange of views," *Packingham v. North Carolina*, 582 U.S. 98, 104 (2017) (citation omitted), they also represent a vital setting for investigative reporting. The "voluminous amount of information" available online "has led to massive shifts in the news industry," and data journalism that leverages new tools to make sense of that information "is now a driving force in newsrooms around the country." D. Victoria Baranetsky, *Data Journalism and the Law*, Colum. Journalism Rev. (Sept. 19, 2018), https://perma.cc/4729-42NP. But as the Supreme Court warned in *Van Buren*, a too-sweeping interpretation of the CFAA would threaten much of that "journalism activity" with the prospect of steep civil and criminal penalties. 593 U.S. at 394.[1]

Take, for instance, the role of scraping—the automated process of pulling large amounts of information from websites—in investigative reporting online.

[1] Because the CFAA is a dual civil-criminal statute, courts "interpret the statute consistently"—applying the rule of lenity, for instance—even if a case involves only civil liability. *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1200 (9th Cir. 2022) (quoting *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004)). As chilling as civil liability can be in its own right, *see Sessions v. Dimaya*, 584 U.S. 148, 183–84 (2018) (Gorsuch, J., concurring in part and concurring in the judgment), amicus also refers to the criminal consequences of the District Court's interpretation of the CFAA in this brief.

Scraping typically does not collect 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). The results, though, after comprehensive data collection and analysis, can reveal much more than any one user visiting the website would have noticed. Journalists have used web-scraping techniques to identify doctors nationwide that have continued to practice after being caught sexually abusing patients, *see* Carrie Teegardin, *Behind the Scenes: How the Doctors & Sex Abuse Project Came About*, Atlanta J.-Const. (Dec. 17, 2016), https://perma.cc/VK7J-QZMG, to evaluate prison conditions, *see* David Eads, *How (and Why) We're Collecting Cook County Jail Data*, ProPublica (July 24, 2017), https://perma.cc/WW69-WKM9, or to shine a spotlight on the national backlog of missing-person cases, *see* Baranetsky, *supra*.

Much of the reporting that leverages scraping relies, in particular, on the use of test accounts, to enable online the sort of "civil-rights testing" that has long played a vital role in exposing unlawful discrimination in brick-and-mortar spaces. *Van Buren*, 593 U.S. at 394. By creating accounts that vary on the basis of race, sex, or other protected characteristics, journalists can aggregate data to compare a

business's responses to different users. That kind of reporting has shown, for instance, that *The Princeton Review* imposed a "tiger mom tax" by listing higher prices for test-prep services in Asian communities, Julia Angwin et al., *The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review*, ProPublica (Sept. 1, 2015), https://perma.cc/TMX7-22N2, and that Airbnb hosts are less likely to accept potential guests with "black-sounding names," Komal S. Patel, Note, *Testing the Limits of the First Amendment: How Online Civil Rights Testing Is Protected Speech Activity*, 118 Colum. L. Rev. 1473, 1474–75 (2018). Other projects rely on users voluntarily sharing access to their own accounts to permit journalists to aggregate information, as in ProPublica's efforts to document targeted political advertising on Facebook. *See* Jeremy B. Merrill, *What We Learned from Collecting 100,000 Targeted Facebook Ads*, ProPublica (Dec. 26, 2018), https://perma.cc/S6PC-NNU9.

Unsurprisingly, the subjects of that sort of reporting would like a license to quash it. *See, e.g.*, Horwitz, *supra* (noting Facebook's cease-and-desist letter to a scraping project that relied on voluntary access to users' accounts). As a result, websites now routinely purport to forbid scraping—or otherwise using the information they host for research purposes—in their terms of service, even as the information remains available to any member of the public who makes an account. *See* Carrero, *supra*, at 134. And on the view the District Court adopted here, if the

CFAA prohibits access to any site that requires the creation of an account once the operator has told a user to stop poking around, *see* J.A. 43, the decision whether to criminalize those routine reporting techniques would rest with the website under investigation. The statute cannot support that reading—one that would raise serious doubts about the Act's constitutional validity. This Court should reject it.

II. The CFAA does not criminalize routine data journalism.

As the Supreme Court explained in *Van Buren*, 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*, 593 U.S. at 389–90. 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 394; *see also id.* at 393 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 beneficial conduct, including routine "journalism activity" and "online civil-rights testing and research." *Id.* at 394.

Under *Van Buren*, the District Court recognized that a user's violation of a purported ban on scraping—a restriction on accessing a computer in a particular manner, or for a particular purpose—cannot itself give rise to CFAA liability. *See* J.A. 34. And the same remains true, the District Court granted, even if an operator purports to instruct a user to stop visiting a website visible to the general public. *See* J.A. 34, 40; *accord hiQ Labs, Inc.*, 31 F.4th at 1195–96. But the District Court reached the surprising conclusion that the result flips if a website requires making an account—even if any member of the public can make one. *See* J.A. 43. That holding makes little sense, and it would present the very same parade of horribles that "underscore[d] the implausibility" of the construction the Supreme Court rejected in *Van Buren*. 593 U.S. at 394.

For one, a typical cease-and-desist letter simply restates the same terms-of-service violation that *Van Buren* held cannot support liability. For just that reason, the Ninth Circuit has observed that letting a site sue based 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' is putting it mildly: In fact, the expedient of simply copying a "purpose-based limit[]" from the terms onto letterhead would eviscerate the guardrails the Supreme Court believed it was establishing. *Van Buren*, 593

U.S. at 396. "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." *Id.* It would do nothing to narrow the "breathtaking amount of commonplace computer activity" that would be punishable *after* making the de minimis effort of sending a letter, *id.* at 393, and it would do nothing substantive to protect "journalism activity" or "online civil-rights testing and research," *id.* at 394, since any platform would be more than happy to take the extra step of sending an email if it would mean avoiding press coverage they see as unfavorable.

Just as importantly, a letter does nothing to draw an intelligible line between "outside hackers" and authorized insiders if the information at issue remains available to any member of the public who makes a free account—and indeed if the user remains (technologically) able to access the website with *their* account. *Van Buren*, 593 U.S. at 389. While *Van Buren* did not ultimately resolve whether the scope of the CFAA "turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies," *id.* at 390 n.8, the Supreme Court made clear that the statute is ultimately directed to "the typical consequences of hacking," *id.* at 392 (citation omitted).[2] "The statutory

[2] In context, footnote 8 is best understood to mean that reference to norms—not just code—is sometimes necessary to distinguish hackers from ordinary computer users. For instance, code alone cannot explain why a journalist is an

definitions of 'damage' and 'loss,'" for instance, "focus on technological harms," *id.* at 391–92, not harms resulting from the alleged misuse of information obtained through ordinary use of a computer, *see id.* But no one would think to describe an individual's continued use of their own, still-functioning password—or the creation of a new account using a website's ordinary process—as hacking.

The canon of constitutional avoidance reinforces that result. For one, the District Court's interpretation presents grave vagueness concerns under the Due Process Clause because it would make "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. Because parties can change their terms of service at any time and for any reason, they can deem criminal behavior that Congress never contemplated when it enacted the CFAA. Requiring that a site send a letter explaining *what* it criminalized on a whim does not fix the problem. Nor does tacking on a cease-and-desist notice reduce the risk that relying on terms of service to define offenses under the CFAA "invites arbitrary enforcement." *Johnson v. United States*, 576 U.S. 591, 595 (2015). That arbitrariness poses a

---

insider when entering her own email password and a hacker when guessing a stranger's; the act of typing in the password is technologically identical in each case. *Cf.* 18 U.S.C. § 1030(a)(6) (prohibiting password trafficking). But the inquiry remains focused on whether the conduct alleged amounts to "hacking," *Van Buren*, 593 U.S. at 392, and while norms may clarify at the margin when entering a password fits that description, entering your *own* password never does.

particular danger for the press, who risk being singled out by, say, an 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*, 587 U.S. 391, 406–07 (2019) (noting that special retaliation concerns are raised by offenses that, like jaywalking, are often committed but rarely charged).

In permitting private parties to outlaw a significant amount of journalism in the public interest, the District Court's interpretation would also raise serious First Amendment concerns. The Constitution, this Court has explained, protects the right "[t]o record what there is the right for the eye to see or the ear to hear." *Fields v. City of Phila.*, 862 F.3d 353, 359 (3d Cir. 2017). Scraping a website on which any member of the public can create an account "is merely a particular use of information that [individuals] are entitled to see," *Sandvig*, 315 F. Supp. 3d at 26–27, 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 15; *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"). But on the District Court's view, whether to criminalize those routine data-journalism techniques is a decision Congress left to each private party that an investigation might offend.

Text and precedent cannot support that conclusion. The CFAA does not prohibit routine "journalism activity," *Van Buren*, 593 U.S. at 394, and interpreting the Act to foreclose those public-interest investigations would severely "limit[] the stock of information from which members of the public may draw," *First Nat'l Bank of Bos. v. Bellotti*, 435 U.S. 765, 783 (1978)—a consequence that Congress cannot reasonably have intended in a statute aimed at "hackers," *Van Buren*, 593 U.S. at 389. Amicus respectfully urges this Court to reject that dangerous result.

CONCLUSION

For the foregoing reasons, the Reporters Committee respectfully urges this Court to affirm the judgment below on the alternative ground that Defendant-Appellee's conduct did not violate the CFAA.

Dated: July 18, 2025

Respectfully submitted,

/s/ Gabe Rottman

Gabe Rottman
Counsel of Record for Amicus Curiae
Lisa Zycherman*
Grayson Clary*
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th St. NW, Suite 1020
Washington, D.C. 20005
Phone: (202) 795-9300
Facsimile: (202) 795-9310
grottman@rcfp.org

**Of counsel*

COMBINED CERTIFICATIONS

I, Gabe Rottman, hereby certify that:

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and 32(a)(7) because the brief contains 2,823 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Office Word in 14-point Times New Roman font.

3. At least one of the attorneys whose names appear on this brief, including the under-signed, is a member of the bar of this Court, as required by Local Rule 28.3(d).

4. The text of the electronic version of this brief is identical to the text of the paper copies to be filed with the Court.

5. The electronic version of this brief filed using the CM/ECF system was virus-checked using Avast Antivirus, and no virus was detected.

Dated: July 18, 2025

/s/ Gabe Rottman
Gabe Rottman
Counsel of Record for Amicus Curiae

CERTIFICATE OF SERVICE

I certify that on July 18, 2025, I caused the foregoing Brief of Amicus Curiae the Reporters Committee for Freedom of the Press in Support of Defendant-Appellee to be electronically filed with the United States Court of Appeals for the Third Circuit using the CM/ECF system. All parties are registered CM/ECF users, and service upon them will be accomplished by the appellate CM/ECF system.

Dated: July 18, 2025

/s/ Gabe Rottman
Gabe Rottman
Counsel of Record for Amicus Curiae