NO. 25-1374

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

RYANAIR DAC,

PLAINTIFF-APPELLANT,

V.

BOOKING COM BV,

DEFENDANT-APPELLEE.

On Appeal from the United States District Court
for the District of Delaware, 1:20-cv-01191
The Honorable William C. Bryson, Circuit Judge

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT- APPELLEE AND AFFIRMANCE

Andrew Crocker
(California State Bar No. 291596)
Kit Walsh
(California State Bar No. 303598)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993
Email: andrew@eff.org

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amicus states that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: July 17, 2025

s/ Andrew Crocker
Andrew Crocker

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Legislative Materials

Other Authorities

STATEMENT OF INTEREST OF *AMICUS CURIAE*[1]

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization with more than 33,000 active donors that has worked for 35 years to ensure that technology supports freedom, justice, and innovation for all people of the world.

INTRODUCTION

Congress enacted the Computer Fraud and Abuse Act to deter harmful attacks on computers and systems. Broadly interpreted, however, it can be a weapon against scrutiny and accountability when well-resourced companies wish to prevent criticism, competition and follow-on innovation. In *Van Buren v. United States* the Supreme Court offered clear guidance rejecting broad readings of the CFAA in favor of careful interpretation tied to its subject: computer hacking. In this context, a technical meaning is a plain meaning.

The district court's interpretation of "without authorization" correctly followed that guidance to conclude that accessing a publicly available website could not violate the CFAA, even when the access might violate the website's terms of use or a cease-and-desist request. However, the court deviated

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), amicus certify that no person or entity, other than amicus curiae, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. Booking consents to the filing of this brief, while Ryanair does not.

significantly from *Van Buren*'s guidance when it held that access tied to use of one's valid username and password might be actionable under the CFAA if the website owner objects to it.

EFF urges this Court to clarify that violations of mere policy, as opposed to hacking of technological security measures, do not qualify as access "without authorization" under the CFAA. This is an alternate ground of affirmance of the order being appealed and would recognize the limits on CFAA liability necessary to protect researchers, journalists, and innovators.

ARGUMENT

I. THE USE OF VALID CREDENTIALS TO ACCESS PUBLICLY AVAILABLE INFORMATION IS NOT "ACCESS WITHOUT AUTHORIZATION"

A criminal statute such as the CFAA needs clear limits, and the Supreme Court provided them in *Van Buren* when it explained that "authorization" in the computer context refers to computer authentication, not a free-wheeling concept of permission. The CFAA does not apply to every person who merely violates terms of service by sharing account credentials with a family member or by withholding sensitive information like one's real name and birthdate when making an account. Rather, the law concerns computer hacking: bypassing a technological restriction on access to a protected computer.

A. The CFAA was not intended to give website owners the power to create criminal liability on their own terms.

The CFAA's historical and statutory context establishes that Congress sought to "prevent intentional intrusion onto someone else's computer—specifically, computer hacking." *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1196 (9th Cir. 2022). Lawmakers were concerned about nightmare scenarios such as the one depicted in the film *WarGames,* where a teenaged hacker breaks into a U.S. military supercomputer and unwittingly nearly starts a nuclear war. The 1984 House Committee Report (incorrectly) stated that the film was a "realistic representation of the automatic dialing and access capabilities of the personal computer." H.R. Rep. No. 98–894, U.S.C.C.A.N. 3689, 3696 (1984).

As a result, Congress passed a 1984 precursor to the CFAA to target serious and malicious computer break-ins. The law was "designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives[.]'" *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130–31 (9th Cir. 2009) (citation to legislative history omitted). The 1984 House Committee Report explained, "the conduct prohibited is analogous to that of 'breaking and entering'"—not "using a computer (similar to the use of a gun) in committing the offense." H.R. Rep. No. 98–894, U.S.C.C.A.N. 3689, 3706 (1984). As an example of that conduct, the Report

pointed to an individual who had "stole[n] confidential software" from a previous employer "by tapping into the computer system of [the] previous employer from [a] remote terminal." *Id*. at 3691–92. The individual would have escaped federal prosecution—despite a clear computer break-in—had he not made two of his fifty access calls from across state lines. *Id*. The Report called for a statutory solution to ensure that such computer intrusions would not evade prosecution.

Two years later, the 1986 CFAA was passed to extend the prohibition on unauthorized access to any "protected computer" under section 1030(a)(2)(C). Again, Congress characterized its intent as prohibiting computer break-ins. *United States v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015). As another example of the conduct targeted by this broadened language, the 1986 Senate Committee Report cited an adolescent gang that "broke into the computer system at [a cancer center] in New York." The group "gained access to the radiation treatment records of 6,000 past and present cancer patients" and thus "had at their fingertips the ability to alter the radiation treatment levels that each patient received." S. Rep. No. 99-432, 1986 U.S.C.C.A.N. 2479, 2480.

It was this sort of technical, exploitative behavior—breaking into a computer system for the purpose of accessing or altering non-public information—that Congress sought to outlaw. It did not intend the CFAA to cover every effort to access a public website without the express permission of a website owner. *Id.* at

2482.

B. The Supreme Court's decision in *Van Buren* directs courts to interpret the CFAA in light of relevant technical definitions.

The Supreme Court's landmark ruling in *Van Buren v. United States* interpreted the CFAA—specifically the terms "exceeds authorized access" and "entitled to obtain"—in light of that intent. *Van Buren v. United States*, 593 U.S. 374, 381-84 ("[W]e start where we always do: with the text of the statute."). The government argued that a law enforcement officer violated the CFAA by accessing a database for purposes that violated his employer's computer use policy. Rejecting that policy-based approach, the Supreme Court looked instead to the "technical meaning[s]" of these terms because "when a statute, like this one, is 'addressing a . . . technical subject, a specialized meaning is to be expected.'" *Id*. at 388 n.7 (internal citation omitted). Thus, for the CFAA, the technical meaning *is* the plain meaning. *Id*. at 388 ("That reading, moreover, is perfectly consistent with the way that an 'appropriately informed' speaker of the language would understand the meaning.") (internal citation omitted).

Accordingly, the Court explained that the phrase "entitled so to obtain" should be construed in the context of computer use, and that this "narrowed scope of 'entitled'" referred to "a computer one is authorized to access." *Id*. at 387. Van Buren had technical authorization to access the computer, and thus the "entitlement" to obtain information from the database for purposes of the CFAA,

regardless of non-technical policies and prohibitions against obtaining the information at issue. In further support of its holding, the majority also relied on the "well established" meaning of "access" in the computing context: "'access' references the act of entering a computer 'system itself' or a 'particular part of computer system,' such as files, folders, or databases." *Id*.

Further, while the majority used a "gates-up-or-down" analogy to describe the statute's prohibitions, it noted that analogy was only useful insofar as it "align[ed] with the computer-context understanding of access as entry." *Van Buren*, 593 U.S. at 390. It is properly understood to address two categories of computer information: (a) information for which authorization is required and has been given, and (b) information for which authorization is required but has not been given. *Van Buren*'s gates analogy stemmed from the CFAA's prohibitions involving "access" and "authorization," which, when interpreted technically, presume an authentication or other system that grants or denies entry. Thus the "gate" is an analogy to that system—so under *Van Buren*, the lack of an authorization system means no gate at all.

Moreover, if the CFAA's prohibition reaches publicly available information that anyone with internet access can view, then the statute would in fact "attach criminal penalties to a breathtaking amount of commonplace computer activity," including web scraping, rather than being "aimed at preventing the typical

consequences of hacking." *Van Buren*, 593 U.S. at 392 (internal citation omitted).

Van Buren also counsels against relying on property law concepts, including analogies to physical trespass, rather than defining authorization according to its technical meaning. The *Van Buren* majority found the dissent's broader interpretation of "entitled," which included circumstance-specific conditions and rested on "basic principles of property law" and "common-law," to be "ill advised," given the CFAA's focus on "computer crime." *Id*. at 384 n.4. A website operator may disable an account it does not wish to continue accessing the site, but writing a letter revoking permission to use an account is not enough to create CFAA liability.

C. Unauthorized access to "private" websites requires circumvention of a technical or "code-based" restriction.

In keeping with *Van Buren's* guidance, the district court correctly understood that a correct reading of the CFAA should not allow private terms of service, contracts, or other communications to control "authorization" to access public websites. Accordingly, the Court should affirm that the CFAA does not forbid access to publicly available information on websites, even if a website owner has attempted to revoke that access with a cease-and-desist letter.

However, the district court erred in concluding that a cease-and-desist letter is enough to support a CFAA claim if a website is password-protected. Unlike "exceeds authorized access," "without authorization" has no statutory definition.

Van Buren's instruction that the CFAA should be interpreted in light of its "technical meaning" should thus apply. *See id*. at 388; *see also hiQ Labs*, 31 F.4th at 1201 (explaining that access "without authorization" requires bypassing "a computer's generally applicable rules regarding access permissions).

Most relevant here, the "CFAA's prohibition on password-trafficking," 18 U.S.C. § 1030 (a)(6), "contemplates a 'specific type of authorization—that is, authentication,' which turns on whether a user's credentials allow him to proceed past a computer's access gate." *Id*. at 390 n.9 (quoting Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 Geo. Wash. L. Rev. 1442, 1470 (2016)). "Authorization," therefore, is not a catch-all term for "permission," but refers to "[a] process by which users, having completed an authentication stage, gain or are denied access to particular resources based on their entitlement." *A Dictionary of Computer Science* 32 (Andrew Butterfield et al eds., 7th ed. 2016). Only by circumventing an authentication stage, then, can someone access a computer "without authorization" in the technical sense. That did not happen here.

The Supreme Court in *Van Buren* explained that "authorization" under the CFAA refers to the computer science concept of authorized access, not to a more general concept of permission. *Van Buren* 593 U.S. at 388. The district court mistakenly believed that the mere *presence* of a technological authorization

measure transformed the computer into one where non-technical *permission* could govern. This is contrary to *Van Buren*'s guidance.

To use the "gates-up-or-down" analogy, if you enter a valid username and password, it is akin to the gatekeeper recognizing you and opening the gates when you ask. The gates, then, are open for you. This scenario is the same as in *hiQ Labs,* where the Ninth Circuit explained, following *Van Buren*, that mere statements of policy or preference are not sufficient to render access "without authorization." 31 F.4th at 1201. It is in no way analogous to taking a battering ram to the gates or picking the lock securing them, the sorts of breaking-and-entering-type hacking activities targeted by the CFAA.

D. Premising liability on non-technological revocation of authorization violates the Rule of Lenity.

Because the underlying statutory prohibition against accessing a computer "without authorization" is criminal, constitutional constraints specific to criminal statutes apply. The district court's interpretation of the CFAA defies these limits.

The Rule of Lenity calls for vague or ambiguous criminal statutes to be interpreted narrowly in favor of the defendant. *United States v. Santos*, 553 U.S. 507, 514 (2008)). It "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).

Concerns about vagueness have been at the heart of multiple decisions to

interpret the CFAA narrowly. *See Van Buren,* 593 U.S. at 390-91*; United States v. Nosal*, 676 F.3d 854, 862–64 (9th Cir. 2012); *Brekka*, 581 F.3d at 1135. Criminal liability based on a computer owner's expression of their preferences would render the statute unconstitutionally vague because it is often unclear when a computer user or website visitor's access becomes access "without authorization," which means the statute may give rise to arbitrary and discriminatory enforcement.

A few examples suffice to demonstrate this ambiguity. Suppose a bank website creates a pop-up notice warning that only credentialed users, not family members, are allowed to access the bank's computer system. Has the person who nonetheless continues to log in with her spouse's legitimate credentials to pay a bill, at the spouse's behest, been given "notice" that her access is "without authorization" under the CFAA? Similarly, could this rule criminalize using a partner's online video streaming account or Amazon account with their permission, if the company started prominently displaying a notice upon each visit to its website that only registered users were allowed to stream videos or order goods, while third parties were not authorized to do so? What about logging into an airline account to print a boarding pass, or paying a bill directly on a utility or credit card website, on behalf of another person? What if the website sent an individual email stating its terms of use? What if it sent a registered letter?

It is common that legitimate credentials are used by account holders or their

agents in ways prohibited by website owners. People often give a password or other access credentials to a family member, caregiver, or other trusted person to allow them to send an email or calendar invitation, check their Facebook or other social networking information or contacts, pay a bill, or check a bank or credit card statement. Predicating "unauthorized access" on the stated wishes of a site owner rather than on technological measures threatens to turn all such "agents" into criminals.

The district court's reasoning thus creates legal uncertainty, rendering ordinary people unable to understand what conduct is prohibited and inviting arbitrary enforcement. *See Mateo v. Atty. General United States*, 870 F.3d 228, 233 (3d Cir. 2017). As the public's use of online services requiring passwords and other forms of authentication prior to access increases, the scenarios for serious criminal liability for innocuous behaviors do, too. And by basing CFAA liability on whether or not a company provided notice that a particular access was unwanted, it repeats the problem the Supreme Court has specifically sought to avoid: imposing criminal liability for violations of computer owners' policies governing how computers are used.

By expanding the scope of CFAA liability in this way, the district court's approach also subjects an untold number of Internet users to prosecution, such that prosecutors can pick and choose which types of password sharing or account

access "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 panel has "invit[ed] discriminatory and arbitrary enforcement." *See Nosal*, 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. To avoid fatal vagueness problems, the CFAA must be narrowly applied to only the behavior Congress clearly intended to criminalize: breaking into computers in order to access or alter information.

II. AN OVERLY BROAD READING OF CFAA LIABILITY THREATENS TO CHILL VALUABLE RESEARCH AND JOURNALISM

The district court's reading of the CFAA also threatens to chill socially valuable research and journalism.

For example, it could potentially criminalize—and therefore undoubtedly chill—investigation of online discrimination. The techniques journalists and academic researchers use to test for such discrimination sometimes require violating specific company prohibitions on certain activities, and are often adversarial to a company's business interests. Offline, audit testing has long been recognized as a crucial way to uncover racial discrimination and to vindicate civil rights laws. *Cf. Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373 (1982).

Online, 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 advertising or housing offers that are displayed to, say, male versus female users. Researchers may also 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 are often adversarial to a company's interests. Pursuant to the district court opinion below, if a company disagrees with the purpose of a researcher's access to its website, it could not only seek to bar such research but can actually render that some of that research criminal by merely sending a letter notifying the researchers that they are not authorized to access its website.[2] Website owners could thereby shut down any unwanted anti-discrimination research or testing, even where the researcher did not break into a computer. Indeed, many researchers already refrain from conducting their socially valuable and constitutionally protected research to avoid the threat of criminal prosecution.[3]

---

[2] *See*, *e.g.*, Knight First Amendment Institute, *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.

[3] *See, e.g.*, Raji and Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products* (Jan. 27, 2019), https://dl.acm.org/doi/10.1145/3306618.3314244. ("researchers who engage in algorithmic audits risk breaching company Terms of Service, the Computer Fraud and Abuse Act (CFAA) or ACM ethical practices … Given these risks, much algorithmic audit work has focused on goals to gauge user awareness of

The problems do not end there. A great deal of computer security research necessarily takes place on systems or software that require users to create accounts. Under the district court's rule, these researchers, too, risk CFAA liability if a company orders them not to access the site. Further, even where computer owners' policies are not fully explicit, researchers' ability to access and use computers may be at odds with the particular means of access the owners believe to be "authorized." If there is no effective technological barrier in place, therefore, users may inadvertently "exceed access" under a broad interpretation of the CFAA merely by accessing computers in an unanticipated manner.

For example, in *United States v. Auernheimer*, 748 F.3d 525, 530-31 (3d Cir. 2014), the defendant was charged with violating the CFAA for demonstrating automated access to thousands of public-facing AT&T websites that the company had not "expected people to find," even though they were accessible to anyone who knew the website addresses—just as a password protected area of a website is accessible to anyone who opens a freely available account.[4] Kerr, *Norms of*

---

algorithmic bias or evaluate the impact of bias on user behavior and outcomes instead of directly challenging companies to change commercial systems.") (citations omitted).

[4] Despite the public accessibility of the AT&T websites, the district court in *Auernheimer* concluded that the indictment "sufficiently allege[d] the elements of unauthorized access." *United States v. Auernheimer*, No. 11-CR-470 SDW, 2012 WL 5389142, at *3 (D.N.J. Oct. 26, 2012), *rev'd on other grounds*, 748 F.3d at 529.

Computer Trespass, 116 Colum. L. Rev. at 1164.

Researchers are hard-pressed to avoid these risks. Almost by its nature, discovering security vulnerabilities requires accessing computers in a manner unanticipated by computer owners, frequently in contravention of the owners' stated policies. The work involves trial and error, as researchers look for vulnerabilities in complex systems. Sometimes researchers employ a chain of techniques that seek to leverage one basic flaw to discover more serious vulnerabilities or demonstrate access to more sensitive data,[5] and often it is the initial stages of their work that involves forms of "access" of uncertain legality.

The Department of Justice itself acknowledges the problem. Recognizing the CFAA and similar laws could be read to criminalize normal "methods of searching for and analyzing vulnerabilities," DOJ's Cyber-Digital Task Force has specifically recommended that the agency adopt explicit carve-outs to "encourage and protect legitimate computer security research" from criminal liability.[6]

Nonetheless, prosecutors continue to interpret the statute broadly. In *United States v. McDanel*, for example, the government brought criminal CFAA charges against a defendant who discovered a security vulnerability, alerted the company,

---

[5] *See, e.g.*, *Privilege escalation*, WIKIPEDIA, https://en.wikipedia.org/wiki/Privilege_escalation.

[6] U.S. Department of Justice, *Report of the Attorney General's Cyber-Digital Task Force* at 110 (2018).

and then, when the company refused to fix the problem, alerted the company's customers.[7] Although the company fixed the bug, the government brought CFAA charges against McDanel for the act of truthfully communicating information about it.[8] As a result, security researchers who discover vulnerabilities must now decide whether disclosing the flaw is worth the risk of inviting a protracted legal battle over their right to speak out. Even when researchers choose to notify a computer owner of a vulnerability, risk of liability under the CFAA may lead them to limit their engagement with the owner, which can make the disclosure process far less effective.

A 2018 in-depth study surveyed twenty academic and independent security researchers with qualitative methods to understand how researchers decide whether to pursue or avoid certain kinds of projects.[9] Half of the subjects reported that they considered the CFAA to be a primary source of risk.[10] More than half of those reported avoiding some or all types of research that might implicate the CFAA.[11]

---

[7] *See* Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1349 (2008).

[8] *Id.* After McDanel appealed his conviction, the government dropped the charges. McDanel had already served eighteen months in prison.

[9] *Id.* at 4.

[10] *Id.* at 9.

[11] *Id*.

The interview subjects noted uncertainty surrounding what activities "exceed authorized access" under the CFAA. As a result, some subjects avoided any potential risk of CFAA liability by avoiding networked systems entirely.[12] Others tried to avoid work that involved terms of service agreements where possible.[13] Several interview subjects stated that they tried to carefully read terms of service, but noted the practical impossibility of doing so at scale—for example, in an Internet-wide network scan.[14] Several researchers experienced retaliation for disclosing vulnerabilities, ranging from verbal and written threats of legal action to FBI investigation in one case, and arrest in another.[15]

To mitigate these risks, many researchers disclose vulnerabilities to an intermediary rather than to companies directly.[16] For example, when MIT researchers uncovered security vulnerabilities in Voatz's mobile voting platform, they sought legal counsel from the Boston University/MIT Technology Law Clinic and disclosed their findings first to the Department of Homeland Security, in part

[12] *Id.* at 9-10.

[13] *Id.* at 10.

[14] *Id.*

[15] *Id.* at 12.

[16] *Id.*

to protect themselves against retaliation.[17]

Others choose to limit their research. For example, researchers studying the security of the Democracy Live Omniballot System, a web-based voting platform that has been used or approved for use in fourteen states and the District of Columbia,[18] they identified security flaws that could allow attackers to alter votes without detection.[19] But they were unable to test comprehensively because "[a]ccessing non-public server functionality might raise legal issues."[20] [21]

To avoid these textbook unintended consequences courts must follow *Van Buren* and interpret the CFAA narrowly, not give website owners a new shield against independent accountability.

---

[17] *See* Abby Abazorius, *MIT researchers identify security vulnerabilities in voting app*, MIT NEWS (Feb. 13, 2020), http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213.

[18] *Approvals, Reviews, and Certifications*, DEMOCRACY LIVE, https://democracylive.com/approvals-reviews-and-certifications/.

[19] Michael A. Specter & J. Alex Halderman, *Security Analysis of the Democracy Live Online Voting System* (June 7, 2020), https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf.

[20] *Id.* at 7.

[21] *Id.*

III. GRANTING WEBSITE OWNERS THE POWER TO TURN THEIR USE PREFERENCES INTO LAW WOULD UNDERMINE COMPETITION.

If unauthorized access can be predicated on a violation of a website owner's stated preferences, rather than hacking technological barriers, then companies will continue to use the CFAA to fend off competition. For example, companies commonly use automated web browsing products to gather web data for a wide variety of uses. Some examples from industry include manufacturers tracking the performance ranking of products in the search results of retailer websites, companies monitoring information posted publicly on social media to keep tabs on issues that require customer support, and businesses staying up to date on news stories relevant to their industry across multiple sources. E-commerce businesses use automated web browsing to monitor competitors' pricing and inventory, and to aggregate information to help manage supply chains. Businesses also use automated web browsers to monitor websites for fraud, perform due diligence checks on their customers and suppliers, and to collect market data to help plan for the future.

Like the companies subject to independent audits and security testing discussed above, some website owners do not welcome automated browsing. If the use of valid credentials in a way that has been disallowed as a matter of stated (or even unstated) policy were a CFAA violation, a company could create a password-

protected "gate," make the key freely available to all, and then send cease and desist letters to anyone they don't like. Again, this concern is not speculative; inhibiting competition is precisely what Ryanair sought to do here, and in keeping with what companies have repeatedly tried to do in the past, with partial success. *See Facebook v. Power Ventures*, 844 F.3d 1058 (9th Cir. 2016) (company that allowed users to login and manage all of their social networking accounts from one place violated CFAA when it allowed users to access Facebook data after it blocked a specific IP address Power was using to connect to Facebook data); *HiQ Labs, Inc. v. Linkedln Corp*. 31 F.4th 1180 (9th Cir. 2022) (platform threatened to bring CFAA claims against a startup company that analyzed the platform's user profiles as part of its business data analytics service, and then promptly began offering its own analytics service); *Southwest Airlines v. Farechase*, 318 F. Supp. 2d 435, 437 (N.D. Tex. 2004) (CFAA claim against price comparison service); *see generally* Charles Duan, *Hacking Antitrust: Competition Policy and the Computer Fraud and Abuse Act*, 19 Colo. Tech. L. J. 313 (2021).[22]

Van Buren marks a turning point in this unfortunate trend by making it clear that CFAA liability turns on technical interpretations of the statute, not merely enforcement of a computer owner's wishes. *Van Buren*, 141 S. Ct. at 1657-58. In

[22] Available at: https://digitalcommons.wcl.american.edu/facsch_lawrev/2176

the context of this case, that means a user with valid credentials is not liable under the CFAA for violating a written contract or ignoring a cease-and-desist letter, because they did not circumvent a technological gate. This Court should affirm the ultimate judgment below on this alternative ground, and in so doing reject the district court's misunderstanding of the scope of the CFAA.

CONCLUSION

For the reasons stated above, this Court should affirm that Booking is not liable under the CFAA.

Dated: July 17, 2025

Respectfully submitted,

*s/ Andrew Crocke*r
Andrew Crocker
(California State Bar No. 291596)

Kit Walsh
(California State Bar No. 303598)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993
Email: andrew@eff.org

Counsel for Amicus Curiae

CERTIFICATE OF BAR MEMBERSHIP

I, Andrew Crocker, am a member in good standing of the bar of the United States Court of Appeals for the Third Circuit and was admitted on April 29, 2014.

Dated: July 17, 2025

s/ Andrew Crocker
Andrew Crocker

CERTIFICATE OF COMPLIANCE

I, Andrew Crocker, counsel for amicus curiae, hereby certify the following statements are true.

The forgoing brief of Amicus Curiae complies with the type-volume limitation of F.R.A.P. 29(a)(5) and 32(a)(7)(B) because this brief contains 4,547 words, excluding the parts of the brief exempted by F.R.A.P. 32(f) and 3d Cir. L.A.R 29.1(b).

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

The text of this electronic brief is identical to the text in the paper copies.

The electronic file of this brief was scanned with antivirus protection program VirusTotal virus protection program has been run on this file and no virus was detected. 3d Cir. L.A.R. 31.1(c).

Dated: July 17, 2025

s/ Andrew Crocker
Andrew Crocker

CERTIFICATE OF SERVICE

I certify that on July 17, 2025, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Third Circuit using the appellate CM/ECF system. All participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: July 17, 2025

s/ Andrew Crocker
Andrew Crocker