No. 19-783

In the Supreme Court of the United States

NATHAN VAN BUREN,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Eleventh Circuit

BRIEF OF AMICUS CURIAE DIGITAL JUSTICE FOUNDATION IN SUPPORT OF AFFIRMANCE

Andrew Grimm
DIGITAL JUSTICE FOUNDATION
15287 Pepperwood Drive
Omaha, NE 68154
(531) 210-2381

Gregory Keenan
DIGITAL JUSTICE FOUNDATION
81 Stewart Street
Floral Park, NY 11001
(516) 633-2633

Edward F. Cunningham
Counsel of Record
LAW OFFICES OF EDWARD F. CUNNINGHAM
62 Cambridge Avenue
Garden City, NY 11530
(516) 328-3705
ed@edcunninghamlaw.com

Counsel for Amicus Curiae

September 3, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF AMICUS CURIAE[1]

The Digital Justice Foundation is a 501(c)(3) nonprofit dedicated to preserving individual rights in digital spaces. The Foundation has particular interest in the impact of digital technologies on civil liberties, personal privacy, individual intellectual-property rights, and individual economic well-being. The Foundation has particular concern for underrepresented users, artists, creators, employees, and innovators, especially those with limited access to law.

The Foundation writes as *amicus curiae* because it believes that there is a threshold matter of whether Petitioner had any entitlement whatsoever. If this Court addresses whether Petitioner had any entitlement whatsoever on the basis of agency law—and the clear rebuke by Petitioner of his agency relationship that was the underlying basis for any claim of entitlement to access a law-enforcement database—it can affirm on narrow grounds. It can, with fidelity to the text and its purpose, thread the needle between providing legal recourse for egregious violations of rights while avoiding the policy catastrophes that so concern many of Petitioner's *amici*.

---

[1] No counsel for any party authored this Brief in whole or in part, and no person or entity other than the *amicus*, its members, or its counsel made a monetary contribution intended to fund the Brief's preparation or submission. All parties have consented to the filing of this Brief.

SUMMARY OF ARGUMENT

The Foundation writes as *amicus curiae* because it believes that the other Briefs present a false binary—between either wholesale gutting the statute's ability to punish the most egregious betrayals by corporate insiders *or* opening Pandora's Box to gross abuses of power by federal prosecutors to imprison whomever they want for innocuous, everyday acts of online behavior.

If those were the only two options, the Foundation would be writing on the other side. It would urge this Court not to put its imprimatur on something like that. Yet the Foundation believes that agency law presents narrow grounds for affirming criminal liability for egregious violations while assuaging concerns of policy catastrophes. We believe that hewing to agency law's longstanding principles offers a route to punish treacherous former agents without criminalizing broad swathes of American society.

What's presented is undoubtedly an important issue. Indeed, the growth of the Internet and its imposition into all facets of everyday life make Internet-law cases highly important, as this Court has astutely observed before. Petitioner's *amici* are right to acknowledge that the digitalization of the economy and all aspects of life makes this case highly important. Yet, that importance does not support their position. The growing importance of online interactions justifies the need for statutes to establish norms online—through well-tailored civil and criminal sanctions. That's why Congress has repeatedly expanded the Act at issue as the Internet has grown.

The Foundation believes that a narrow affirmance based on agency law is the best way forward. In fact, this Court could establish an agency-based rule here that holds Petitioner accountable while avoiding criminalizing vast swathes of American society. It is Petitioner's loss of his status as an agent based upon egregious acts against his employer's interest that explains why he was not entitled to access the database when he did. Applying this approach would faithfully apply the text, fulfill its purpose, avoid outrageous consequences, and still recognize the fundamental importance of rights online.

Emphatically, most Americans do not betray their employers. Mild deviation from corporate policy minutiae does not abrogate agency relationships *ipso facto*. By contrast, Petitioner-style violations certainly do—beyond a reasonable doubt. Thus, this Court can affirm on the narrow grounds of agency—distinguishing trivial violations of a human-resources policy handbook from genuine and egregious betrayals of employers' interests.

For these reasons, the Foundation respectfully submits this Brief as *amicus curiae* and urges that this Court affirm on the narrow ground of agency.

ARGUMENT

I. THE INTERNET'S GROWING PREVALENCE SINCE 1986 MAKES THE ACT'S PROTECTIONS MORE IMPORTANT, NOT LESS SO.

1. In 1986, Congress enacted the key defined phrase at the heart of this appeal: "exceeds authorized access." Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213. Much has changed since 1986, but the importance of the CFAA's protections against unauthorized uses of computerized information remains firmly entrenched.

2. Many *amici* have powerfully described just how different the world looks today as compared to 1986. For example, one *amicus* points out that, in 1986, there were merely "2,000 total networks connected via the Internet[.]" Nat'l Assoc. Crim. Defense Lawyers Cert. *Amicus* Br. 8. Today, there are "nearly 50 billion network connected devices[.]" Id.

3. Without a hint of hyperbole, the Electronic Frontier Foundation observes that "it would be difficult to go a single waking hour, let alone a single day, without using the Internet and thereby connecting to someone else's computer system[.]" EFF Cert. *Amicus* Br. 4. Given this huge expansion of computerized information into every corner of life, it is only natural that the CFAA has become ranked amongst "the most far-reaching criminal laws in the United States Code." Id. at 3.

4. But whereas these *amici* argue that the rise of computer usage and the Internet cuts against the CFAA's value, we see it differently.

5. To us, the digitalization of all aspects of life serve to make the CFAA's protections all the more important. The CFAA protects both the privacy and property interests of everyday citizens in their computerized information.

6. The CFAA's protections reflect Congress' efforts "to affirm the government's recognition of computerized information as *property*." S. Rep. No. 99-432, at 14 (1986) (emphasis added). Now today, the average citizen carries around a prodigious portfolio of such property in her pocket: "Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day." Riley v. California, 573 U.S. 373, 395 (2014). "Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception." Id.

7. This Court has "recognized the 'immense storage capacity' of modern cell phones[.]" Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018). Indeed, "the term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers[.]" Riley, 573 U.S. at 393. These minicomputers perform a dizzying array of function, serving as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." Id.

8. Moreover, the deeply intimate nature of this computerized information adds to the public interest in having the CFAA's protections against unauthorized uses. Today "more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." Riley, 573 U.S. at 395.

9. Such computerized information carries tremendous "consequences for privacy." Id. at 394. Individuals' smartphones and personal computers often contain "every picture they have taken[.]" Id. at 393. And the interests in keeping this private information private are sizeable: "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions[.]" Id. at 394.

10. Computerized information provides "an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations" as well. Carpenter v. United States, 138 S. Ct. 2206, 2217-2218 (citation omitted).

11. In short, these ubiquitous computer technologies "hold for many Americans the 'privacies of life.'" Riley, 573 U.S. at 403.

12. Petitioner and some of his *amici* think this contemporary technological milieu renders the statute possibly "obsolete[.]" See, e.g., Petitioner's Br. 31. In fact, the opposite is true. Today, computerized information is a form of property owned by a far wider class of citizens than ever before.

13. Such technological and social realities make the CFAA's protections of computerized information unprecedentedly important to ordinary citizens. The Act advances the public's property rights and privacy interests. And, the CFAA's importance is poised to grow. With each passing day, "every segment of our society becomes increasingly connected[.]" Tech. Companies *Amicus* 5. The continued "explosion of personal computing devices" drives the continued "seamless interconnection of our personal, financial, and professional lives online." Petitioner's Br. 16.

14. Against this dizzying backdrop of accelerating digital technologies enters this dispute about the meaning and scope of the CFAA. Petitioner and his *amici* worry that affirmance here would criminalize "whole categories of otherwise innocuous behavior" and would subject "most everyone who uses a computer" to criminal liability. Petitioner's Br. 26-27 (citation omitted). If that were true, then we would respectfully urge this Court to reverse. We think that's a false binary; the text of the statute permits this Court to apply quite ordinary principles of agency law, to narrowly affirm, and to limit this case to similar facts showing egregious betrayal of an employer.

15. Moreover, Petitioner and his *amici* overlook that ordinary citizens find themselves with interests on both sides of this kind of dispute. Ordinary citizens are constantly accessing and using computerized information. But they are also possessors and owners of computerized information—an ever-growing amount.

16. Importantly, affirming here on narrow grounds would not have disastrous consequences. Most citizens are not hackers and would never dream of using their work computers to sabotage their employers. Most employees do not use their work computers to subvert the very purposes of their principal or employer. Thus, the vast majority of citizens stand to lose nothing by affirmance in cases like the one here, if affirmed on narrow grounds of agency that require violations to reach the level of *ipso facto* terminating the agency relationship's very entitlements and leaving lesser issues outside its criminal scope.

17. Thus, this *amicus* brief advocates for an agency approach to interpreting the Act's concept of entitlement that simultaneously enforces its text, fulfills its purpose, and avoids *amici*'s worries. The public interest lies decidedly in robust protections of this computerized information—without catching innocent behaviors too.

18. Today, the computerized information that the CFAA was designed to protect no longer rests in some remote corner of the electronic frontier. Today, such computerized information permeates the heartland of everyday daily life. The CFAA is thus all the more important in this increasingly "interconnected world[.]" See EFF Cert. *Amicus* 3.

II. AN AGENCY APPROACH SUPPORTS AFFIRMANCE ON THE NARROW GROUNDS THAT AGENTS LOSE AGENCY-BASED ENTITLEMENTS WHEN THEY UNDERTAKE EGREGIOUS ACTS THAT TERMINATE THEIR AGENCY.

1. In our view, Petitioner is correct on many points of statutory interpretation about the scope and meaning of the key statutory words at issue: "not entitled so to obtain[.]"

2. Nonetheless, Petitioner overlooks a threshold issue. *Even if* this Court agrees with Petitioner on nearly every issue of statutory interpretation, longstanding principles of agency support a narrow affirmance that Petitioner was "not entitled so to obtain" information from the Georgia Crime Information Center's database because, before he did, he had terminated the underlying agency relationship upon which his entitlement to do so depended.

3. Petitioner decided to serve another—one whose ostensible purpose was entirely antithetical to the purpose of Petitioner's law-enforcement role generally and database access specifically. Then, Petitioner took acts that manifested serious disloyalty to his police department. In so doing, he himself rebuked the very role upon which his access to the database depended. And, since he did all this *before* he queried the database, Petitioner was no longer entitled to query the database whatsoever. At that point in time, he was hacking the database.

4. Critically, though, it's a tall order to end an agency relationship by acts alone. No mere frolic and detour, nonchalance toward corporate policies, or pure laziness will do. Instead, it's manifestations of directly adverse interest that cross the line.

5. Petitioner makes a number of compelling points about the Act. For one, Petitioner is correct that the pertinent provisions, 18 U.S.C. § 1030(a)(2), (e)(6), do not turn on his subjective purpose at the time that he accessed the relevant database.

6. Section 1030(a)(2) has no purpose requirement whatsoever in its text. After scouring the U.S. Code books, Petitioner rightfully points out that that improper-purpose requirements do, in fact, exist "elsewhere" in other Titles of the Code but are notably absent from Section 1030(a)(2), (e)(6). Petitioner's Br. 19. We think Petitioner could have stayed closer to home: Section 1030(c)(2)(B)(i) ups the ante by heightening criminal penalties if "the offense was committed for *purposes* of commercial advantage or private financial gain[.]" 18 U.S.C. § 1030(c)(2)(b)(i) (emphasis added). As a result, this statutory inclusion of a purpose-requirement somewhere else in the same section is indicia that the key provision here does not turn on a mere improper purpose. Congress knew how to use purpose requirements.

7. Furthermore, we think that the Government's reliance on the word "so" in "entitled *so* to obtain or alter" is misplaced. See Gov't Br. 13, 18-19. The word "so" does not fundamentally alter the scope of liability. Rather, it plays a specifying function.

8. By comparison, consider how Section 1030(e)(6) says "**a** computer" but then shifts to the phrase "information in **the** computer[.]" 18 U.S.C. § 1030(e)(6). Notice that it does so in order to *specify* that the computer containing the information must be the same as the one that was accessed. The phrase "**a** computer" clarifies that it can be any computer (as defined) and, in turn, the phrase "**the** computer" specifies the computer accessed must be the same one with the information in it.

9. So too with the word "so" in the phrase "entitled *so* to obtain or alter[.]" See id. The word "so" has a specifying function. The phrase "entitled *so* to obtain or alter" ties the issue of entitlement back to the specific "access to obtain or alter" that preceded it. The word "so" is how a reader knows that the access used to obtain or alter the information and the entitlement to undertake that access are necessarily connected. Thus, the word *so* is "pivotal"—just not as the Government would like. See United States v. Markiewicz, 978 F.2d 786, 804-805 (2d Cir. 1992) ("Defined as 'such as has been specified or suggested', Webster's Third New International Dictionary 2160 (1971), the word 'so' […] refers back[.]").

10. In addition, we agree with Petitioner's astute illustration about the hypothetical loan officer who wishes to improperly use credit-history reports to overzealously advertise additional services. Petitioner's Br. 18. An ordinary speaker would not say that the officer's subjective purpose eliminated the entitlement to access the information. Id.; see Cert. Petition 17 (similar but slightly different example).

11. Thus, we too agree that entitlement is binary as the statute sees it. You either have an entitlement to use access to obtain certain information—or you don't. You either have the entitlement to alter certain information in a certain way[2]—or you don't.

12. Then, there's the issue of *entitlement*. At the time he last accessed the database, Petitioner didn't have any entitlement to access that information. That's the flaw in Petitioner's argument. On these facts, Petitioner did not access the database for merely "inappropriate reason[s]" or, after he got the information, perform a "simple misuse or misappropriation of information." Petitioner's Br. 13, 17. Instead, his acts preceding his access rebuked the agency relationship upon which his entitlement to access the database was entirely dependent.

13. Petitioner says the "ordinary meaning of the word 'entitle' is 'to give a right.'" Petitioner's Br. 18. Therefore, to Petitioner, a "person is thus 'entitled so to obtain' information when she has the right, via some prescribed manner, to acquire that information." Id. Thus, the question is whether Petitioner

---

[2] Notably, alteration of information is more complicated. Generally speaking, there is only one way to obtain information from a computer. But, there are unlimited numbers of ways to alter a piece of information. It's possible that an employee might be entitled to update information, but not delete it wholesale because those are *different* alterations. Regardless, if employees are entitled to update a calendar, for example, their subjective purpose as they go about the update is not a talisman of liability.

had the right to acquire information from the database at the time that he did.

14. And his was no inalienable right of access to that information. It was contingent upon his status as an agent of the police department.

15. Although Petitioner had not formally resigned his position, turned in his badge, or stopped receiving his department's payroll, he didn't need to in order to terminate his agency relationship: "[T]he authority of an agent terminates if, *without knowledge of the principal*, he acquires adverse interests or if he is otherwise *guilty of a* ***serious*** *breach of loyalty to the principal*." Maples v. Thomas, 565 U.S. 266, 284 (2016) (emphasis added) (quoting Restatement (Second) of Agency). A minor breach will not do.

16. Here, Petitioner "commit[ed] a breach of duty [of loyalty] to his principal by acting for another in an undertaking which has a substantial tendency to cause him to disregard his duty to serve his principal with only his principal's purposes in mind." See id. (second set of brackets in original). Petitioner's conduct meets the high bar of "disloyalty or renunciation of his role, which *would* terminate [his] authority[.]" See Holland v. Florida, 560 U.S. 631, 668 n.9 (2010) (italics in original).

17. Critically, an "agent is not deemed to have acted adversely to his principal's interests simply because he blundered and made an unwise, negligent, or grossly negligent mistake that harmed those interests." Cadet v. Fla. Dep't of Corr., 853 F.3d 1216, 1229-1230 (11th Cir. 2017). Yet Petitioner's loss of

entitlement does not stem from failing to follow every arcane rule in his department's dusty policy rulebook.

18. Rather, Petitioner made a series of conscious choices to take on interests that are entirely antithetical to his role as agent of a police department. Emphatically, Petitioner's activities were not everyday activities. Thus, affirming on the narrow ruling that he surrendered the rights he had *ex officio* through his status as a law-enforcement agent couldn't "transform everyday activities into federal crimes[.]" Petitioner's Br. 15.

19. Petitioner is correct that "Employer-employee and company-consumer relationships are traditionally governed by tort and contract law." Petitioner's Br. 25 (quoting Nosal). Yet, *employer-employee* relationships—unlike company-consumer relationships—are also typically governed by *agency* law. Maples, 565 U.S. 266, 284 ("Hornbook agency law"); see also Petitioner's Br. 21 ("hornbook law"). Indeed, it is agency law's features on the "legal landscape" that confirm it is appropriate to affirm because agency law's very focus is determinations of authority (apparent and actual) and entitlements thereunder. And, the Act's key words implicate those concepts in a way that relates to an agent's authorization.

20. Although they are not limited to them and a different approach of contractual or situational authorization would apply outside of the principal-agent context, agency law's specific focus on these kinds of relationships and betrayals go to the fundamentals determining this issue.

21. Nor is turning to general agency law a foreign concept in interpreting a federal statute that uses words that implicate agency concepts. Cf. Cmty. for Creative Non-Violence v. Reid, 490 U.S. 730, 750-751 (1989) ("To determine whether a work is for hire under the [Copyright] Act, a court first should ascertain, using principles of general common law of agency[.]"); cf. Cmty. for Creative Non-Violence v. Reid, 846 F.2d 1485, 1494 n.11 (D.C. Cir. 1988) (Ginsburg, J.) (same).

22. It is also important to note that termination-of-agency decisions are questions of fact that juries must decide in particular circumstances. Thus, a determination on agency grounds *is* a narrow ruling and in future cases would need to be proven beyond, as with all jury issues in criminal cases, beyond a reasonable doubt and would be sufficiently nuanced to turn on issues related to the sophistication of the criminal (or civil) defendant. See Restatement (Second) of Agency § 112, Comment b ("Whether or not the disloyalty of the agent is such that he should realize that the principal would desire the termination of his entire authority at once is a question of **fact**." (emphasis added)).

III. THE PROPOSED AGENCY APPROACH AVOIDS THE POLICY CATASTROPHES THAT PETITIONER AND *AMICI* FEAR.

1. There are two animating hypothetical policy concerns motivating Petitioner's narrow reading of the CFAA. The proposed agency approach to interpreting the CFAA helps assuage such worries. Indeed, this Court could use the proposed agency approach to distinguish the present case from Petitioner's hypotheticals and affirm here, while leaving line drawing exercises for another day Or, if it so chooses, this Court could employ the proposed agency approach to draw a sensible, middle-of-the-road line that precludes Petitioner's hypotheticals from CFAA liability while still affirming here. The Court could either distinguish entirely based on agency grounds or use the agency approach to draw a clear limiting principle.

A. The proposed agency approach avoids criminalizing innocuous violations of workplace web-browsing policies.

2. *First*, Petitioner raises the concern that using a workplace computer for personal uses, such as leisure time web-browsing at work, could lead to criminal convictions under the CFAA. To illustrate this worry Petitioner presents his March Madness example. Petitioner's Br. 28. Petitioner discusses hypothetical employees checking March Madness basketball scores on a work computer. To Petition, such conduct would "likely violate their employers' policies prohibiting using 'work computers for personal purposes.'" Id.

3. Petitioner alleges that "this activity is also a felony" if its reading of the CFAA is not adopted. Id. We don't agree.

4. Petitioner's March Madness example would implicate the first prong of 18 U.S.C. §1030(a)(2) ("access a computer without authorization"). However, the present case raises an interpretive question under the second prong of 18 U.S.C. §1030(a)(2) ("exceeds authorized access"). Whereas the first prong focuses on authorization to a (workplace) computer, the second prong focuses on an entitlement to information. Per the definition of 18 U.S.C. §1030(e)(6), to exceeds authorized access "means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

5. Suppose an employee uses a popular sports website, say ESPN, to check basketball scores while at work in violation of company policy. The information obtained does not reside on the company's computer. Rather the information is obtained from *ESPN's server*. See Petitioner's Br. 27 ("host server").

6. The information is made publicly available by ESPN to the Internet at large via ESPN's publicly available servers. Therefore, the avid fan checking basketball scores *is* entitled to the information; the public at large is. Fans' obtaining of information from ESPN servers is between them and ESPN. And, ESPN is more than happy to have the web traffic, even from distracted workers.

7. Even if checking sports scores violates the company's internal policies, it is not the company's information and so the company does not determine who is or is not entitled to the information publicly available online from ESPN.

8. In short, per Section §1030(e)(6)'s definition, the "exceeds access to authorize" prong of an 18 U.S.C. §1030(a)(2) claim is an information-based offense. The employee's relationship to the proper owner of that information (here ESPN) would determine whether he was entitled to obtain that information.

9. If there is a CFAA claim for Petitioner's March Madness example it would need to lie in the first prong of a § 1030(a)(2) claim ("access a computer without authorization"). But such a benign, commonplace violation of workplace internet rules would not likely automatically revoke authorization to use the workplace computer and it certainly wouldn't do so *ipso facto* under agency law. Employees of a company are authorized to use their workplace computers and do so as an agent of their principal. Revoking computer access entirely could not even be assumed to be in the principal's interest: after all, the reason for those policies is presumably productivity. Taking away computer access would presumably harm productivity.

10. Tangential or non-productive uses of company time are no employer's dream, but checking sports scores is not so antithetical to the purpose of the agency as to result in the *ipso facto* revocation of agency.

11. Thus, several probably insurmountable bars would need to be cleared in order to support a conviction under the CFAA for personal web-browsing of sport scores while at work. First, the conduct would need to be so egregious a betrayal or so antithetical to the principal's purpose that it would sever the agent relationship inherently via the conduct. That's a high bar. For example, to most of this Court, even an attorney's failure to communicate in a timely fashion to a client does not *ipso facto* sever the agency relationship. See Holland 560 U.S. at 668 n.9. Checking sports scores almost assuredly wouldn't either.

12. *Second*, the government would need to prove beyond a reasonable doubt that the conduct itself severed the agent relationship as a matter of agency law. Finally, the tacit approval and implied consent of many bosses around the country that turn a blind eye to—or even encourage—the cultural phenomenon of March Madness would make it all the more unlikely that such a situation poses any genuine cause for concern of a CFAA violation.

13. Moreover, in the civil context, a CFAA claim would also need to prove damages of at least $5,000 resulting from the employee checking sports scores.

14. The question is whether you lost authorization to your work computer entirely by the mere act of violating company policy to browse in the workplace.

B. The proposed agency approach avoids criminalizing trivial breaches of websites' terms of service.

15. Petitioner raises a terms of service worry. Petitioner's Br. 28. Petitioner observes that "virtually every public website or internet-based application contains terms of service." Id. Petitioner suggests that the commonplace practice of exceeding such terms of service could "exceed authorized access" in violation of the CFAA, thereby criminalizing commonplace conduct.

16. As a threshold matter, such a case is entirely distinguishable from the present case because such a terms of service case does not involve an agency relationship, but rather a purely contractual relationship. No matter how much time an internet user might spend on Instagram or streaming Netflix, they do not become an agent of that service provider and do not owe that service provider a duty of loyalty.

17. Thus, affirming here using the proposed agency approach, would allow affirmance on narrow grounds without delving into the distinct issues raised by terms of service and breach of contract cases.[3]

---

[3] Also, the agency approach would address the circuit split on how the CFAA should treat employees who exceed the scope of permitted uses of information. See United States v. Valle, 807 F.3d 508, 525 (2d Cir. 2015); United States v. Van Buren, 940 F.3d 1192, 1197–98 (11th Cir. 2019). One *amicus* has suggested that these results demonstrate "indefensible inconsistencies" in how the CFAA is applied. Nat'l Assoc. Crim. Def.

18. Further, a violation of the terms of service often does not result in the automatic loss of entitlement to the information, pursuant to §1030(e)(6). For example, Petitioner cites the eBay terms of service regarding eBay's Duplicate listings policy. Petitioner's Br. 29 n. 6. But, if one reads those terms of service, it becomes clear that a violation of these terms does not terminate an eBay user's entitlement to access the eBay platform. In pertinent part, those terms of service read: "Activity that doesn't follow eBay policy ***could*** **result** in a range of actions including **for example**: administratively ending or canceling listings, hiding or demoting all listings from search results, lowering seller rating, buying or selling restrictions, and account suspension."[4]

19. In short, a violation of a term of service is not a self-executing revocation of an entitlement to use that service or to obtain information from that service.

Cert. *Amicus* 4. But where that *amicus* sees "indefensible inconsistencies," an agency approach could see a nuanced difference. An agency approach allows one to distinguish between an employee's unauthorized browsing that merely exceeds the scope of an employee's authorized use—which would not revoke an agent's entitlement—and an employee's unauthorized browsing that is antithetical to the employer's purposes—which would sever the agent relationship and revoke entitlement as a matter of agency law.

[4] eBay, Duplicate listings policy, at https://perma.cc/8WTZVDHT (emphasis added).

20. Instead, a violation of terms of service would present breach-of-contract questions. Such a breach would not necessarily terminate any contractual relationship between the parties. Indeed, a "breach does not terminate a contract as a matter of course [.]" Whitney Inv. Co. v. Westview Dev. Co., 273 Cal. App. 2d 594, 602 (1969).

21. Moreover, as a practical matter password sharing is an open secret to companies like Netflix. If companies turn a blind eye to password sharing, such companies may be acquiescing or tacitly accepting such behavior by their users even if they have language to the contrary buried in their terms of use. The contract law significance of such practices would be a matter of state law.

22. In short, it is not at all clear that, as a matter of contract law, a violation of a company's terms of service would revoke a user's entitlement to obtain information on that company's website *ipso facto* without a specific revocation directed to the user. And again, this Court need not wade into such contract analysis here. The present case involves a CFAA violation in an employment context that is best dealt with by the proposed agency law approach.

CONCLUSION

This Court should affirm but on the narrower grounds that Petitioner's acts had terminated his agency relationship and, with it, any entitlement to access a proprietary law-enforcement database.

Respectfully submitted,

Andrew Grimm
DIGITAL JUSTICE FOUNDATION
15287 Pepperwood Drive
Omaha, NE 68154
(531) 210-2381

Gregory Keenan
DIGITAL JUSTICE FOUNDATION
81 Stewart Street
Floral Park, NY 11001
(516) 633-2633

Edward F. Cunningham
Counsel of Record
LAW OFFICES OF EDWARD F. CUNNINGHAM
62 Cambridge Avenue
Garden City, NY 11530
(516) 328-3705
ed@edcunninghamlaw.com

Counsel for Amicus Curiae

September 3, 2020