No. 19-783

IN THE
Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES,

Respondent.

On Petition for a Writ of Certiorari to the
U.S. Court of Appeals
for the Eleventh Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND FIFTEEN TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF RESPONDENT

ALAN BUTLER
Counsel of Record
MEGAN IORIO
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
butler@epic.org

September 3, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C.[1] EPIC was established in 1994 to focus public attention on emerging civil liberties issues, to promote government transparency, and to protect privacy, the First Amendment, and other constitutional values.

EPIC filed an *amicus curiae* brief in support of the petition for a writ of certiorari in *LinkedIn v. hiQ Labs*, which is currently pending before the Court. Brief of Electronic Privacy Information Center as *Amicus Curiae* in Support of Petitioner, *LinkedIn Corp. v. hiQ Labs, Inc.,* No. 19-1116 (filed Apr. 13, 2020). EPIC also participated as *amicus* in the proceedings below. Brief for EPIC as *Amicus Curiae* in Support of Appellant, *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019) (No. 17-16783).

EPIC routinely files *amicus* briefs in this Court concerning the interpretation of privacy statutes. *See, e.g.*, Brief for EPIC et al. as *Amici Curiae* Supporting Petitioners, *Barr v. Am. Ass. of Political Consultants*, No. 19-631 (U.S. filed Nov. 14, 2019) (arguing that the Telephone Consumer Protection Act is constitutional); Brief for EPIC as *Amicus Curiae* Supporting Respondents, *PDR Network v. Carlton & Harris Chiropractic*, 139 S. Ct. 2051 (2019) (No. 17-1705) (arguing that TCPA defendants should not be able to challenge FCC

---

[1] Both parties consent to the filing of this brief. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

interpretations of the TCPA outside the review process Congress established); Brief for EPIC et al. as *Amici Curiae* Supporting Respondent, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (No. 13-1339) (arguing that violation of statutory privacy rights confers Article III standing); Brief of EPIC et al. as *Amici Curiae* Supporting Petitioner, *Maracich v. Spears,* 570 U.S. 48 (2013) (No. 12-25) (arguing that the scope of the litigation exception to the Driver's Privacy Protection Act should be narrow); Brief for EPIC et al. as *Amici Curiae* Supporting Petitioners, *Sorrell v. IMS Health*, 564 U.S. 552 (2011) (No. 10-779) (arguing that a Vermont law restricting use of prescriber-identifying data protected patient privacy); Brief for EPIC as *Amicus Curiae* Supporting Petitioners, *Reno v. Condon*, 528 U.S. 141 (2000) (No. 98-1464) (arguing that the Driver Privacy Protection Act was consistent with constitutional principles of federalism).

EPIC's brief is joined by the following distinguished experts in law, technology, and public policy:

Legal Scholars and Technical Experts

Anita L. Allen
Henry R. Silverman Professor of Law, Professor of Philosophy, University of Pennsylvania

Ann Bartow
Professor of Law, University of New Hampshire Franklin Pierce School of Law

Christine L. Borgman
Distinguished Research Professor & Director, UCLA Center for Knowledge Infrastructures

Danielle Keats Citron
Professor of Law, Boston University School of Law; Vice President, Cyber Civil Rights Initiative

Addison Fischer
Founder, Verisign Inc.

Jerry Kang
Distinguished Professor of Law and Asian American Studies, Inaugural Korea Times—*Hankook Ilbo* Endowed Chair, Founding Vice Chancellor of Equity, Diversity, and Inclusion, UCLA

Len Kennedy
EPIC Scholar-in-Residence

Chris Larsen
Executive Chairman, Ripple Inc.

Harry R. Lewis
Gordon McKay Professor of Computer Science, Harvard University

Gary T. Marx
Professor Emeritus of Sociology, MIT

Dr. Pablo Garcia Molina
Assistant Vice President, Chief Information Security Officer, Drexel University

Rashida Richardson
Visiting Scholar, Rutgers Law School

Jim Waldo
Gordon McKay Professor of Computer Science, Harvard University

Christopher Wolf
Board Chair, Future of Privacy Forum

Shoshana Zuboff
Charles Edward Wilson Professor of Business Administration, Emerita, Harvard Business School

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, protects the confidentiality, integrity, and security of computer data and networks. As originally enacted in 1984, Section 1030(a)(2) established protections for personal data stored in computer systems described in two of the major privacy statutes of the 1970s, the Right to Financial Privacy Act, 12 U.S.C. §§ 3401 et seq., and the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq. Congress subsequently expanded the scope of the provision to extend data protections to other types of computer systems. But the underlying purpose of Section 1030(a)(2) never changed. Indeed, Congress recognized as it expanded the scope of Section 1030(a)(2) in subsequent amendments the unique threats posed by Government employees exceeding their access privileges to obtain sensitive and confidential information. That is precisely what happened in this case and there is no ambiguity that the CFAA applies here.

It is true, as many of the other *amici* emphasize, that technology has advanced dramatically in the nearly thirty years since the CFAA was enacted. But as the capacity to collect, store, and analyze data has grown exponentially, so have the risks to privacy. Government databases, in particular, now hold vast quantities of some of the most sensitive personal data imaginable. Government computer systems can limit an individual's freedom to travel, can impact their ability to seek employment or credit, can restrict their access to healthcare and other essential benefits, and can even place them under the microscope of a law enforcement inquiry. The potential damage that can be caused by improper access to these systems is

immense. We need the CFAA, now more than ever, to be an extra check against abuse by the people entrusted to access sensitive data and systems.

On the other side, many interested *amici* groups and scholars argue that the CFAA should be read "narrowly" in order to avoid expansive liability. But the scenarios that they describe bear no resemblance to this case, and their arguments are based on an arbitrarily limited view of what the law prohibits. There is no basis in the text or history of the CFAA to conclude that the law only applies when individuals circumvent code-based or technical controls on access to protected computers or government systems. Quite the contrary. Code-based restrictions are designed to prevent outsiders from breaking into a system; they do not adequately protect against unauthorized access by insiders who already have some access. The term "exceeds authorized access," which is defined in the statute, clearly refers to the type of insider threat that Congress intended to prohibit. In this case a police officer improperly ran searches of personal information in a criminal database for financial gain. That is a paradigmatic example of an individual exceeding their authorized access to a system and there should be no ambiguity that such actions violate the CFAA.

The case does not require a broad proclamation of how the CFAA applies in the Internet context, nor does it demand a resolution of theoretical cases that have never been charged. And even if the statute does have implications for data scraping, research, and other protected activities, there is still no reason to distinguish between code-based and contract-based access restrictions. Any limiting principle should be tethered to the underlying purpose of Section 1030(a)(2),

to protect sensitive data from exposure and subsequent misuse. To the extent the Court is interested in addressing the enforcement of code-based and contract-based restrictions on the scraping of data from public-facing websites, that issue would be better addressed by granting the pending petition in *LinkedIn v. hiQ Labs*.

ARGUMENT

I. The CFAA protects sensitive personal data and should be interpreted consistent with that purpose.

Congress enacted and subsequently expanded Section 1030(a)(2) of the CFAA to protect personal information stored in recordkeeping systems. The scope of Section 1030(a)(2) should be co-extensive with its data protection purpose. On the one hand, there is no textual, historical, or data protection reason to exclude non-technical access restrictions from the scope of Section 1030(a)(2). Limiting liability to circumstances where an individual bypasses an authorization gate would effectively eliminate the "exceeds authorized access" prong of the provision and greatly undermine the law's data protection purpose. It is not practical to rely on code-based access restrictions to implement the protections necessary for all modern databases. In many situations a mix of code-based and rule-based access restrictions strike the best balance between privacy and practicality and provide sufficient notice of the applicable standards. On the other hand, it would not serve CFAA's data protection purpose to apply Section 1030(a)(2) to situations where there is no legitimate privacy or confidentiality interest in the data accessed.

A. Section 1030(a)(2)(C) was enacted, and later expanded, by Congress to protect sensitive data from both outsider and insider threats.

The history of Section 1030(a)(2) shows that Congress was concerned with preventing improper access to protected *information*—specifically, *records* kept by the owner of a computer system. The provision was originally enacted to protect from improper access highly sensitive, individually identifiable financial information covered by the Financial Privacy Act and the Fair Credit Reporting Act, two important financial privacy statutes. 18 U.S.C. § 1030(a)(2) (Supp. II 1984); *see also* H.R. Rep. No. 98-894, at 21 (1984). The Financial Privacy Act prohibits the federal government from obtaining customer records collected and stored by a financial institution except under limited circumstances. 12 U.S.C. §§ 3401 et seq. Similarly, the Fair Credit Reporting Act prescribes the circumstances under which records collected and stored by consumer reporting agencies can be obtained. 15 U.S.C. §§ 1681 et seq. Section 1030(a)(2) extended these data privacy rights by prohibiting *anyone* from obtaining the protected information unless authorized.

The 1986 amendments reinforced the data protection purpose of Section 1030(a)(2) and marginally broadened the scope of information protected by the provision. The Senate report noted that the "premise" of the provision was "the protection, for privacy reasons . . . of sensitive and personal financial information." S. Rep. No. 99-432, at 6 (1986). Whereas the Financial Privacy Act had only protected information of customers who were individuals or partnerships with five or fewer partners, the amendments

"extend[ed] the same privacy protections" to the financial data of all customers. *Ibid*.

The Senate report for the 1996 amendments—which led to the broadest expansion of Section 1030(a)(2)—repeatedly stressed that Congress's focus was on protecting sensitive information stored in computerized recordkeeping systems. The report observed that the "privacy protection coverage of the statute"—Section 1030(a)(2)—had "two significant gaps": the statute did not cover "information held on any civilian or State and local government computers" and only prohibited outsiders, not insiders, from obtaining "information held on Federal Government computers." S. Rep. No. 104-357, at 4 (1996). The expansion of Section 1030(a)(2) was meant to "increase protection for the privacy and confidentiality of computer information" by covering insiders who abused their access to obtain information stored on federal computers and those who sought access to information on computers used in interstate commerce. *Id*. at 7.

Some of the other *amici* suggest that the Court should interpret the CFAA's prohibitions to apply only where code-based access restrictions were circumvented. *See, e.g.*, Br. of Professor Orin S. Kerr as *Amicus Curiae* in Support of Petitioner at 7. But this reading would be inconsistent with the text and purpose of the statute. Congress was clear that the law was meant to prohibit malicious access by outsiders ("without authorization") and by insiders ("exceeds authorized access"). *See* S. Rep. No. 104-357, at 6–7. Congress also added or removed liability for insiders through various amendments, so where Congress left "exceeds authorized access" language, it intended to target the conduct of insiders. *See* S. Rep. No. 104-357, at 4, 7

(describing the need to prohibit insiders from improperly accessing private data in federal computers); S. Rep. No. 99-432, at 7–8 (removing the "exceeds authorized access" language from the intra-departmental prong of Section 1030(a)(3) to exclude insiders from liability but retaining the language in Section 1030(a)(2)). Limiting liability to violations of code-based restrictions would read the phrase "exceeds authorized access" out of the statute and make it impossible to punish officials who improperly use their credentials to access sensitive personal data.

B. The CFAA's prohibition on exceeding limits on authorization to access personal data is consistent with data protection principles.

The CFAA's provisions should be interpreted in line with the Fair Information Practices ("FIPs")—data protection principles upon which federal data privacy statutes like the Privacy Act, 5 U.S.C. § 552a(e), are based. These principles call for restrictions on the purpose for which personal information may be collected and limitations on subsequent uses. U.S. Dep't of Health, Education, & Welfare, *Records, Computers and the Rights of Citizens* (1973) [hereinafter HEW Report];[2] *see also, e.g.,* 5 U.S.C. § 552a(b) ("Conditions of Disclosure"); 47 U.S.C. § 551(c) ("Protection of subscriber privacy – Disclosure of personally identifiable information"). Section 1030(a)(2)(C) clearly prohibits access that exceeds the authorized purpose and is in line with the FIPs and other standards that were developed in parallel to the CFAA. These prohibitions

[2] https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

are necessary to enforce data protection principles because it is often impossible or impractical to create a code-based barrier that can enforce purpose specifications. The proposed interpretations offered by Petitioner and his *amici* would undermine a key data protection aim of the statute.

In 1973, a report by the Department of Health, Education, and Welfare (the "HEW Report"), first articulated the FIPs and recognized that access restrictions were key to preventing data misuse. The report described threats from both outsiders who obtained "unauthorized access" to records and insiders who used "authorized access for unauthorized purposes." HEW Report. The authors of the report were primarily concerned about the latter because "most leakage of data" from systems containing personally identifiable information appeared "to result from improper actions of employees either bribed to obtain information, or supplying it to outsiders under a 'buddy system' arrangement." *Ibid.* To help "detect improper dissemination of personal data," the authors of the report recommended that organizations "maintain a complete and accurate record of every access to and use made of any data in the system, including the identity of all persons and organizations to which access has been given." *Ibid.*

The original language of Section 1030(a)(2) mirrored the HEW Report and explicitly prohibited insiders from using their authorization to access information for some purposes to obtain data "for purposes to which such authorization does not extend." 18 U.S.C. 1030(a)(2) (Supp. II 1984). The House report contrasted this unauthorized purpose access with access "for a legitimate business purpose." H.R. Rep. No.

98-894, at 21. Congress replaced the "cumbersome" purpose language with the "exceeds authorized access" phrase not to change the underlying aim of the statute but to "simplify the language" of the provision. S. Rep. No. 99-432, at 9.

Almost every state legislature has also recognized that employees who access and use data for improper purposes breach the security of their computer systems. The data breach statutes of the District of Columbia and every U.S. state except Connecticut and Mississippi contain an exemption for the "good-faith acquisition of personal information" by an employee provided that the information is obtained for the purpose of the employer or not used for an improper purpose. *See* Ala. Code § 8-38-2; Alaska Stat. § 45.48.050; Ariz. Rev. Stat. § 18-551(1)(b); Ark. Code Ann. § 4-110-103(1)(B); Cal. Civ. Code § 1798.82(d)(3)(g); Colo. Rev. Stat. § 6-1-716(1)(h); Del. Code Ann. tit. 6 § 12B-101(1)(a); D.C. Code § 28-3851(1)(B)(i); Fla. Stat. § 501.171(1)(a); Ga. Code Ann. § 10-1-911(1); Haw. Rev. Stat. § 487N-1; Idaho Code § 28-51-104(2); 815 ILCS 530/5; Ind. Code § 24-4.9-2-2(b)(1); Iowa Code § 715C.1; Kan. Stat. Ann. § 50-7a01(h); Ky. Rev. Stat. Ann. § 365.732(1)(a); La. Stat. Ann. § 51:3073(2); Me. Stat. tit. 10, § 1347(1); Md. Code Ann., Com. Law § 14-3504(a)(2); Mass. Gen. Laws ch. 93H, § 1(a); Mich. Comp. Laws § 445.63(b); Minn. Stat. § 325E.61(d); Mo. Rev. Stat. § 407.1500(1); Mont. Code Ann. 30-14-1704(4)(a); Neb. Rev. Stat. § 87-802(1); Nev. Rev. Stat. § 603A.020; N.H. Rev. Stat. Ann. § 359-C:19(V); N.J. Stat. Ann. § 56:8-161; N.M. Stat. Ann. § 57-12C-2(D); N.Y. Gen. Bus. Law § 899-aa(c); N.C. Gen. Stat. § 75-61(14); N.D. Cent. Code § 51-30-01(1); Ohio Rev. Code Ann. § 1349.19(A)(1)(b); Okla. Stat. tit. 24, § 162(1); 73 Pa. Stat. § 2302; 11 R.I. Gen. Laws § 11-49.3.3(a)(1);

S.C. Code Ann. § 39-1-90(D)(1); S.D. Codified Laws § 22-40-19(1); Tenn. Code Ann. § 47-18-2107(1)(B); Tex. Bus. & Com. Code § 521.053(a); Utah Code Ann. § 13-44-102(1)(b); Vt. Stat. Ann. tit. 9, § 2430(12)(B); Va. Code Ann. § 18.2-186.6(A); Wash. Rev. Code § 19.255.005(4); W. Va. Code § 46A-2A-101(1); Wis. Stat. § 134.98(2); Wyo. Stat. Ann. § 40-12-501(a)(i). The existence of these exemptions indicates that employees who access information for an improper purpose breach the security of the system.

A recent example of Twitter employees who accessed private Twitter user data in violation of Twitter policies illustrates the urgent need to deter insiders from improperly accessing personal information held by their employers. In 2015, two Twitter employees allegedly accessed over 6,000 user accounts and relayed personal information about several anonymous and pseudonymous Saudi dissident accounts, including email addresses, phone numbers, and IP addresses, to the Saudi government. Ryan Gallagher, *Spies in Silicon Valley: Twitter Breach Tied to Saudi Dissident Arrests*, Bloomberg (Aug. 19, 2020).[3] At least five of the Saudi Twitter users were subsequently arrested by the Saudi government. *Id.* At least one of the Twitter employees may have had credentials that allowed them to access the user data, but because of his role in the company, he had "no legitimate business purpose" for accessing the accounts. Complaint at ¶ 63, *United States v. Abouammo, et al.,* No. 3:19-71824 (N.D. Cal. filed Nov. 5, 2019). Twitter's Playbook policies for employees prohibited employees from accessing users'

[3] https://www.bloomberg.com/news/articles/2020-08-19/twitter-security-breach-blamed-for-saudi-dissident-arrests.

private data unless required by their job duties. *Id.* at ¶ 23.

Authorization gates and other code-based restrictions could not prevent this type of misuse because employees and other "insiders" do require access to data for legitimate purposes. Under the Petitioner's proposed interpretation of the CFAA, for example, the state of Georgia would need to create a new access credential each time a law enforcement officer needed to run a license plate through the GSIS database and individually vet each request based on the officer's stated purpose for accessing the record. The administrative costs would be astronomical. In circumstances where employees need routine access to a database, it is far more practical and economical to enforce an access policy, formally train officers on the limits of proper use, and track the records accessed, than micromanage each access attempt.

II. The CFAA is an important tool to enforce restrictions on access to personal information stored in government databases.

Government employees have access to vast troves of highly sensitive personal information stored in government databases. The employees may require access to this information to perform their job duties. But government employees have a responsibility not to use their access credentials to view the information for purposes outside the scope of their duties. Improper access is a well-documented problem, particularly among law enforcement officers who have access to databases that contain the personal records of millions of Americans nationwide. Administrative penalties are often not a sufficient deterrent to this sort of abuse. Prosecution under the CFAA and other

computer crimes statutes is thus an important tool to deter insider threats and protect personal data.

Government databases store highly sensitive personal information. For example, the Department of Homeland Security maintains several databases that hold individuals' names, Social Security numbers, dates of birth, addresses, telephone numbers, citizenship information, gender, occupation, driver's license information, credit card numbers, travel itineraries, and criminal histories. U.S. Dep't of Homeland Security, *U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy* 3–4 (Sep. 13, 2019);[4] U.S. Dep't of Homeland Security, Privacy Impact Assessment for the Citizenship and Immigration Data Repository 10–12 (Jan. 3, 2017);[5] U.S. Dep't of Homeland Security, *Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing* 8 (Dec. 22, 2010).[6] The State Department's Consular Consolidated Database, which is the centralized database for U.S. visa and passport services, contains the names, birthdates, Social Security numbers, nationality, medical information, passport information, arrests and convictions, and family information for all U.S. passport and visa holders. U.S. Dep't of State, *Privacy Impact Assessment*: *Consular*

---

[4] https://www.cbp.gov/sites/default/files/assets/documents/2020-May/PNR-Privacy-Policy-%28508-Compliant%29.pdf.

[5] https://www.dhs.gov/sites/default/files/publications/privacy-pia-031-a-uscis-cidr-may2017.pdf.

[6] https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf.

Consolidated Database 3 (Oct. 2018).[7] The Department of Housing and Urban Development also stores names, Social Security numbers, dates of birth, addresses, ethnicity, gender, spousal information, number of children, income, employment history, and disability information in its Tenant Rental Assistance Certification System to confirm tenant eligibility for HUD services. U.S. Dep't of Housing & Urban Development, *Tenant Rental Assistance Certification System Privacy Impact Assessment* 8 (Apr. 2009).[8] The Farm Service Agency's Direct Loan System at the Department of Agriculture stores many of the same types of information protected by the very first enactment of Section 1030(a)(2) , including names, Social Security numbers, financial information, farm production information, assets, and liabilities. U.S. Dep't of Agriculture, *Privacy Impact Assessment Direct Loan System* 3 (June 30, 2009).[9] Similarly, the Department of Education collects the personal and financial information for millions of students and their parents every year through the Free Applications for Federal Student Aid ("FAFSA") system. U.S. Dep't of Education, *Privacy Impact Assessment for FAFSA on the Web* 2–3 (July 7, 2008).[10] The National Institute of Health's Clinical Research Information System contains sensitive health data, including names, Social Security numbers, medical notes, height, weight, medications administered, and services provided. U.S. Dep't of Health & Human

---

[7] https://www.state.gov/wp-content/uploads/2019/05/Consular-Consolidated-Database-CCD.pdf.

[8] https://www.hud.gov/sites/documents/DOC_15042.PDF.

[9] https://www.usda.gov/sites/default/files/documents/FSA_Direct_Loan_System_(DLS)_PIA.pdf.

[10] https://www2.ed.gov/notices/pia/fafsa.pdf.

Servs., *Privacy Impact Assessment: Clinical Research Information System* 2 (Sep. 26, 2016).[11] State and local agencies store similar data.

Government databases increasingly store some of the most sensitive personal information, including biometric data such as fingerprints, facial recognition templates, and DNA profiles. *See, e.g.,* U.S. Dep't of State, *Privacy Impact Assessment*: *Integrated Biometric System* 1–2 (2018) (storing biometrics for facial recognition);[12] Fed. Bureau of Investigation, *Privacy Impact Assessment for the Next Generation Identification (NGI) Palm Print and Latent Fingerprint Files* (Jan. 20, 2015) (storing palm prints and fingerprints);[13] Fed. Bureau of Investigation, *Privacy Impact Assessment National DNA Index System (NDIS)* (Feb. 24, 2004) (storing DNA profiles).[14] Those who improperly access biometric data can create fraudulent copies of the biometric traits to mislead a biometric sensor or identify their biometric doppelganger—someone who shares enough biometric traits to trick a biometric sensor. Nat'l Res. Council, Nat'l Academies, *Biometric Recognition* 50 (Joseph N. Pato & Lynette I. Millett eds. 2010). Because biometrics are becoming a routine method of authentication, the individual can then use the biometric data to access even more sensitive personal information through a biometric authentication

---

[11] https://www.hhs.gov/sites/default/files/nih-clinical-research-information-system.pdf.

[12] https://www.state.gov/wp-content/uploads/2019/05/Consular-Consolidated-Database-CCD.pdf.

[13] https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/next-generation-identification-palm-print-and-latent-fingerprint-files.

[14]

gate. Such is the constant fear of the 5.6 million individuals whose fingerprints were stolen in the Office of Personnel Management's massive 2015 data breach. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2020).[15]

Law enforcement officers have access to particularly extensive databases of sensitive personal information. The National Crime Information Center ("NCIC") is one such information clearinghouse maintained by the FBI and accessible to "virtually every criminal justice agency nationwide." Fed. Bureau of Investigation, *National Crime Information Center (NCIC)* (2020).[16] The persons files in the NCIC store information such as individuals' names, gender, race, Social Security number, driver's license and license plate numbers along with issuing state, passport information, email addresses and other internet identifiers, fingerprint data, photographs, physical and medical characteristics, and other descriptive information. Fed. Bureau of Investigation, *Privacy Impact Assessment for the National Crime Information Center (NCIC)* 3 (Mar. 12, 2019).[17] Access to the database is only authorized for specific law enforcement purposes such as apprehending fugitives, solving crimes, and locating missing persons. *Id*. at 2.

Yet a report by the Associated Press found many instances of inappropriate access by police to NCIC and other law enforcement databases Sadie Gurman, *AP: Across U.S., Police Officers Abuse Confidential*

---

[15] https://www.opm.gov/cybersecurity/cybersecurity-incidents.

[16] https://www.fbi.gov/services/cjis/ncic.

[17] https://www.fbi.gov/file-repository/pia-ncic.pdf/view.

Databases, AP (Sep. 28, 2016).[18] The AP collected records on hundreds of instances across the country where police improperly accessed personal information in law enforcement databases over a two-year period. *Ibid*. The AP noted that record keeping inconsistencies made it "impossible to know how many violations occur" and called its tally "unquestionably an undercount." *Ibid.* The incidents documented included police who accessed personal information for the purpose of stalking an ex-girlfriend, running checks on a journalist who ran unflattering stories about the department, and looking up the phone numbers or home addresses of romantic interests. *Ibid*. The report noted that "officers are only occasionally prosecuted, and rarely at the federal level" due to the unsettled interpretation of the CFAA. *Ibid.*

Other investigations have revealed further information about the problem at the state and local level. In California, for instance, more than 1,000 law enforcement officers were found to have improperly accessed the California Law Enforcement Telecommunications System ("CLETS") in the last decade. Sam Stanton et al., *More than 1,000 California Police Accessed Background Check Database for Personal Use*, Sacramento Bee (Nov. 14, 2019).[19] Some of those prosecuted included an officer who ran background and DMV checks on tenants renting his girlfriend's apartments; another who accessed information on a romantic rival and then drove out to key her car; and yet another who accessed information about two people involved in a lawsuit against him and then issued them

---

[18] https://apnews.com/699236946e3140659fff8a2362e16f43.
[19] https://www.sacbee.com/news/investigations/article237091029.html.

a series of fake traffic and parking tickets. *Ibid.* In an especially egregious case, police officers improperly accessed information about a police board member and allegedly used the information to execute a traffic stop. Thomas Peele, Kensington Cops Used Confidential Database to Gather Information on Police Board Member, KQED (Feb. 20, 2019).[20] The board member called the improper access and subsequent stop harassment. *Ibid.* Another victim of improper access said: "It's such a clear-cut thing. You're not allowed to do that." Stanton et al., *supra*. But prosecutions for improper access in California are rare: only 54 of the over 1,000 officers found to have improperly access the database had charges filed against them. *Ibid.*

The 2015 annual report of Denver's civilian police oversight agency documented 25 officers who accessed law enforcement databases, including the NCIC, for improper purposes such as stalking—but none were prosecuted. Nicholas E. Mitchell, *2015 Annual Report*, Denver Office of the Independent Monitor (2016).[21] The agency's independent monitor stated that "reprimands that are generally imposed on DPD officers who misuse the databases do not reflect the seriousness of that violation, and may not sufficiently deter future misuse." *Id*. at 10. Other jurisdictions have also reported troubling cases of police improperly accessing personal information in law enforcement databases. *See, e.g.* Louise Matsakis, *Minnesota Cop Awarded $585K After Colleagues Snooped on Her*

---

[20] https://www.kqed.org/news/11727412/kensington-cops-used-confidential-database-to-gather-information-on-police-board-member.

[21] https://www.denvergov.org/content/dam/denvergov/Portals/374/documents/2015AnnualReport_OIM.pdf.

DMV Data , Wired (June 21, 2019);[22] Niraj Chokshi, *Florida Officer Spent Years Abusing Police Database to Get Dates, Authorities Say*, N.Y. Times (Mar. 11, 2019);[23] Tess Sheets, *12 Orlando Police Officers Disciplined for Misusing Driver's License Database*, Orlando Sentinel (Feb. 14, 2019);[24] Benjamin Weiser, *Retired Police Sergeant Pleads Guilty to Tapping Into Confidential Databases for Money*, N.Y. Times (Feb. 26, 2016);[25] Kim Zetter, *Female Cop Gets $1 Million After Colleagues Trolled Database to Peek at Her Pic*, Wired (Nov. 5, 2012).[26]

The lack of robust and enforceable restrictions on government employee access to sensitive personal information undermines public trust in the government. Indeed, back in 1973, the HEW Report declared that "concern about abuses of authorized access" to data systems maintained by governments "can have a particularly debilitating effect on people's confidence in their governmental institutions." HEW Report. More recently, the Denver independent monitor noted that "misuse of [law enforcement] databases for

---

[22] https://www.wired.com/story/minnesota-police-dmv-database-abuse/.

[23] https://www.nytimes.com/2019/03/11/us/florida-cop-dating-women.html.

[24] https://www.orlandosentinel.com/news/breaking-news/os-ne-orlando-police-david-misuse-investigation-20190212-story.html.

[25] https://www.nytimes.com/2016/02/27/nyregion/retired-police-sergeant-pleads-guilty-to-tapping-into-confidential-databases-for-money.html.

[26] https://www.wired.com/2012/11/payout-for-cop-database-abuse/.

personal, non-law enforcement purposes may compromise public trust." Mitchell, *supra*, at 10.

III. Criminalizing improper insider access to sensitive personal data does not lead to a slippery slope.

Petitioner and many of his *amici* make different versions of the same slippery slope argument: if the Petitioner's conduct was criminal then other conduct that is important, innocent, or innocuous would be criminalized. There is no doubt that many of the activities discussed in these briefs are laudable and that journalists, researchers, and ordinary internet users should not be subject to criminal liability for harmless conduct. But this case is easily distinguishable from those examples. The slippery slope arguments fail for two reasons. First, this case involves a Government employee accessing sensitive personal information about citizens in knowing violation of policies of his agency and unambiguously falls within the ambit of the CFAA. Second, this case involves a traditional database used to store personal information, not a website or other public-facing computer system, and therefore liability is consistent with the underlying data protection purpose of the statute. The question of whether an individual exceeded their authorized access to obtain information from a protected computer will depend on the specific facts at issue in each case and the norms underlying the CFAA.

First, this case is distinguishable from all of the examples presented by Petitioner and *amici* because it involves improper access to personal data on a Government computer system. Some of the amici have raised concerns about how restrictions imposed by private entities might shape the scope of criminal penalties

under the CFAA. *See, e.g.,* Br. of *Amicus Curiae* Americans for Prosperity Foundation in Support of Petitioner. That argument is beside the point in this case; the restrictions at issue were established by the state of Georgia and the federal government. There is no serious argument that Petitioner lacked fair notice of the restrictions on his access to the Georgia Crime Information Center or the National Crime Information Center databases or that the access restrictions were illegitimate. Petitioner received formal training on proper and improper access and, by his own admission, knew that accessing the information was "wrong." *United States v. Van Buren*, 940 F.3d 1192, 1208 (11th Cir. 2019), *cert. granted*, No. 19-783 (U.S. Apr. 20, 2020). And even in circumstances where an individual violates the CFAA by exceeding access restrictions imposed by a private company, there is no reason why it would be illegitimate for the CFAA to enforce contract-based access restrictions but legitimate for the CFAA to impose code-based restrictions. Just because word-based restrictions are written in prose instead of code does not make them more like a law than code-based restrictions. Both code-based and word-based restrictions are set by the entity that controls a computer system and define the boundaries of authorization to access information on that system. When that entity is a Government agency and the data at issue is sensitive personal information, the violation falls squarely within the scope of what Congress sought to prohibit under the CFAA.

Second, this case is distinguishable from many of the examples offered by Petitioner and *amici* because it involves a traditional database used to store sensitive personal information; it does not involve access to a public-facing website on the internet. There

is no reason why the decision in this case should dictate the outcome in hypothetical future cases involving CFAA claims about routine internet use. The fact that other circumstances could theoretically present difficult or problematic CFAA claims does not negate the fact that the conduct at issue in this case clearly violated the statute.

Further, Section 1030(a)(2) is not concerned with just any access to a computer but access to *information* maintained by the computer owner, and the restriction at issue should be a restriction on access to *that* information and serve a legitimate data protection purpose. This case involves just such a restriction: the defendant improperly accessed personal information and thereby violated restrictions meant to protect the privacy of citizens' personal data—a legitimate data protection purpose. The Court should make clear that when access restrictions serve a legitimate data protection purpose, they can be enforced through the CFAA regardless of whether they are implemented through code or contract.

Several of the *amici* raise concerns about the application of the CFAA to data scraping, but those concerns are very far afield from this case. *See, e.g.,* Br. of *Amici Curiae* Kyratso Karahalios, et al., in Support of Petitioner; Br. of *Amicus Curiae* The Markup in Support of Petitioner; Br. of The Reporters Committee for Freedom of the Press et al. as *Amici Curiae* Supporting Petitioner. Data scraping could be limited by either code- or contract-based access restrictions or, as is commonplace, a mix of both. Sometimes a data scraping restriction will serve a legitimate data protection purpose, such as when it protects personal data from unexpected and unauthorized uses. In other cases,

data scraping restrictions might serve impermissible anticompetitive or anti-accountability purposes. The pending petition in *LinkedIn Corp. v. hiQ Labs, Inc.*, No. 19-1116, squarely presents the legal questions involved in applying the CFAA to data scraping, and the Court should grant the petition to resolve these questions. But data scraping is not at issue in this case and the Court does not have the necessary factual and legal context to address it here.

The panoply of difficult or problematic CFAA hypotheticals offered by the Petitioner and *amici* do not implicate the data protection concerns raised by the conduct at issue in this case. We agree that the Court should be wary of adopting a broad interpretation that would criminalize the types of conduct that the other *amici* describe. But it is not difficult to distinguish this case from those examples. This case does not involve charges against an employee who violates a general computer use policy by browsing the web for non-business purposes. *See* Br. of Professor Orin S. Kerr as *Amicus Curiae* in Support of Petitioner at 5, 26. This case also does not involve a situation like the one in *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), where the defendant was accused of violating a restriction on entering false data into a social media platform. *Id.* at 454; *see also* Br. of Professor Orin S. Kerr as *Amicus Curiae* in Support of Petitioner at 18–23. Neither of those examples involve restrictions on access to information *maintained by the controller* of the computer system and neither implicate data protection concerns.

Just as there are many distinct code-based restrictions, there are many different types of word-based restrictions on computer access. The term

"access a computer" is exceedingly broad and encompasses several distinct concepts. Entering data in a database is a separate act from accessing the same data, so restrictions on the types of data that can be entered on a computer can be distinguished from restrictions on access to the same information on the computer. Restrictions on access to information can be further distinguished from restrictions that generally regulate use of the computer. Finally, some restrictions are reasonably aimed at protecting the privacy and confidentiality of data maintained by the computer owner, while other restrictions have no legitimate data protection purpose.

Indeed, scholars who have studied how the CFAA applies to conduct on the internet have recognized that judges must necessarily weigh competing norms in each case based on the facts presented. *See, e.g.,* James Grimmelmann, *Consenting to Computer Use*, 84 Geo. Wash. L. Rev. 1500, 1514, 1516, 1518 (2016); Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum L. Rev. 1143, 1147 (2016). So even in cases involving violations of code-based access restrictions it would not be possible to generalize across different factual scenarios. The same should hold for cases involving violations of contract-based restrictions. *See* Grimmelmann, *supra*, at 1514. Determinations about whether violations of particular access restrictions fall within the scope of the CFAA will depend on the facts and competing norms implicated in each case. Many scholars and advocates will argue that courts should prioritize open access norms. *See* Kerr, *Norms of Computer Access, supra*, at 1161 . But, for the reasons articulated above, we believe that data protection norms should also guide the interpretation of the CFAA. In the vast majority of cases, like in this case, those

interests will not be in tension. But each case will need to be decided based on its specific facts and circumstances, and there is no doubt that the conduct at issue in this case violates the CFAA.

CONCLUSION

For the above reasons, *amicus* EPIC respectfully asks this Court to affirm the judgment of the U.S. Court of Appeals for the Eleventh Circuit.

Respectfully submitted,

ALAN BUTLER
MEGAN IORIO
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
(202) 483-1248 (fax)
butler@epic.org

September 3, 2020