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 THE FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION AS *AMICUS CURIAE* IN SUPPORT OF RESPONDENT

JOSEPH V. DEMARCO
Counsel of Record
DAVID M. HIRSCHBERG
ERIC SEIDEL
BRIAN A. FOX
DEVORE & DEMARCO LLP
99 Park Avenue, Suite 1100
New York, NY 10016
(212) 922-9499
(917) 576-2369
jvd@devoredemarco.com

Counsel for Amicus Curiae

August 31, 2020

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES—Continued

OTHER AUTHORITIES Page(s)

TABLE OF AUTHORITIES—Continued

INTEREST OF *AMICUS CURIAE*[1]

The Federal Law Enforcement Officers Association ("FLEOA"), a volunteer organization founded in 1977, is the largest nonpartisan, nonprofit professional association exclusively representing federal law enforcement officers. FLEOA represents more than 28,000 uniformed and non-uniformed active and retired federal law enforcement officers from over 65 different agencies. FLEOA is a charter member of the Department of Homeland Security Federal Law Enforcement Advisory Board; holds two seats on the Congressional Badge of Bravery Federal Board; and serves on the Executive Board of the National Law Enforcement Officers Memorial Fund and the National Law Enforcement Steering Committee. FLEOA provides a legislative voice for the federal law enforcement community and monitors legislative and other legal issues that may impact federal law enforcement officers.

Due to the highly sensitive work conducted by FLEOA members, the security of the data they rely upon is paramount. Advances in technology have greatly assisted modern law enforcement agencies by increasing the efficiency, accuracy, and responsiveness of their efforts. No technology has been more important to the administration of law enforcement than computer systems. The systems in use by law enforcement today range from relatively mundane recordkeeping software to sophisticated programs and databases that allocate and direct law enforcement's

---

[1] Pursuant to Supreme Court Rule 37.6, no counsel for a party authored this brief in whole or in part. No person or entity other than the Federal Law Enforcement Officers Association and its members made any monetary contribution to fund the preparation or submission of this brief. The parties have consented to this filing.

resources. The information stored on and accessible through the IT systems operated by federal law enforcement agencies is no less important. It includes, among other data, a staggering amount of sensitive and confidential information concerning ongoing investigations and agency plans and procedures. In performing their duties to protect and serve the public, FLEOA members rely on these IT systems and databases every day. As such, FLEOA is well aware of the dangers that would result should the information contained in those systems be subject to unauthorized dissemination, alteration, or deletion. Perhaps in no single other area would the administration of justice in this country be so corrupted than if federal law enforcement computer systems were to be rendered unavailable or unreliable.

For those reasons, FLEOA — recognizing that the Computer Fraud and Abuse Act ("CFAA") is the primary federal statute which criminalizes malfeasance in relation to federal law enforcement's computer systems — is substantially invested in ensuring that the CFAA is interpreted in a manner which fully protects the accuracy, reliability, and security of its computer systems and databases.

SUMMARY OF ARGUMENT

Since being enacted in 1986, the Computer Fraud and Abuse Act has been the most visible and effective federal law to combat cybercrime. While the CFAA criminalizes a variety of cybercrimes, the majority of the prohibited acts require that an individual access a computer either "without authorization" or by "exceed[ing] authorized access." The CFAA defines "exceeds authorized access" as "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)),

but the seemingly more basic term "authorization" is left without any explicit statutory definition. As a result of this circumstance, differing interpretations of the term "authorization" will either *bolster* criminal protections of vital law enforcement databases or severely *undermine* them.

It should be noted that this confusion does not apply in instances where an "outsider" — that is, someone who has no legitimate access to a computer system for any purpose — accesses a federal database. The CFAA is quite clear when applied to the circumstances of an outside "hacker" who uses technological tools and methods to "break into" a system and thereby steal data or commit cyber-vandalism. Although that situation may be the one most thought of as prototypical by those without significant experience in the field of computer security, those with such experience are all too well-aware that the threat to systems by "insiders" — those who have been granted, as a technological matter, the ability to use a computer system — is at least as, and in many cases more, significant than the threat from outsiders. Countless examples from both the public and private sectors demonstrate that individuals who routinely access shared computer resources in their day-to-day jobs are quite often the perpetrators of crimes targeting data contained on those systems or the operation of the systems themselves.

It is in the realm of this "insider" threat that application of the CFAA has become muddled. Under the current state of the law, there is uncertainty as to whether the provisions of the CFAA which contain the element of "unauthorized" activity are to be read as referring merely to the *technological* provision of access credentials to a system or data, or

whether other factors — such as policy or contractual restrictions — should also be considered when evaluating the nature of an individual's activity on a computer system.

FLEOA respectfully submits that an interpretation of the CFAA that, as Petitioners maintain, considers only the issue of technological controls would be disastrous to the security of sensitive law enforcement computer systems and databases. This is because a regime where the only relevant question is "*could* the defendant have accessed this data without resorting to 'hacking' activities" would allow any person who has legitimate access to the data carte blanche to access and use (or indeed in many cases destroy) that data for any manifestly blameworthy reason they choose. Such a regime therefore renders limited-use grants of access meaningless.

Put another way, Petitioner's reading of the law shifts the blame from the person who commits a data theft or vandalism to the system's overseer for failing to implement technological measures to stop the thief or vandal. To analogize to the physical world (as is often useful in the analysis of abstract computer security questions), Petitioner's interpretation is akin to a rule of law that states "if you give a key to your neighbor so they can water your plants while you are on vacation, you cannot prevent them from going through your medicine cabinet and stealing your jewelry as well." This reading contradicts the plain and common understanding of what it means to engage in "unauthorized" conduct. It also makes no sense.

Worse still, from a practical perspective, a purely technological interpretation of "authorization" in the CFAA would present law enforcement with a dilemma. On the one hand, they could choose to administer and

maintain those systems in a manner which allows legitimate users the greatest freedom to conduct their work efficiently — but risk insider abuse of those systems and forego any criminal legal recourse for that misuse by those insiders. Alternatively, they could frantically attempt to "lock down" access controls to those systems so as to retain the possibility of criminal recourse — but, in the process, render the systems inefficient to maintain, far more costly in terms of financial and human resources, and removing much of their cross-platform efficacy and intelligence-sharing functionality.

FLEOA proposes that the only way out of this quandary is by according "unauthorized access" its plain, common-sense meaning. We therefore respectfully submit that the operator of a system, as the owner of that property, has the right to determine what each user of the system is permitted to do on that system. FLEOA further submits that, when the scope of that access is clearly delineated to the user, the scope of authorization is what controls for a violation of the statute; "authorization" is that which has been granted by the system owner and no more. Particularly in the context of non-public systems containing highly sensitive, confidential and non-public data used daily by law enforcement, FLEOA maintains that the objectives of the CFAA — to protect computerized systems and data from theft, malicious destruction, and attacks which render those systems unusable — are more reasonably met when the scope of "authorized" activity is determined by considering the totality of the circumstances of the grant of access against the plain meaning of the statute, and not merely the dry technological controls employed.

ARGUMENT

I. AN INTERPRETATION OF THE CFAA WHICH ONLY FOCUSES ON THREATS FROM OUTSIDE "HACKERS" IGNORES THE REALITY OF HOW MODERN COMPUTER SYSTEMS, INCLUDING THOSE USED BY LAW ENFORCEMENT, OPERATE

A. Computerized Systems Used by Federal Law Enforcement Agents and Officers Are Repositories of Massive Amounts of Highly Sensitive Information

Like most modern organizations, federal law enforcement agencies rely heavily on computerized systems to fulfill their core mission of protecting the public and the Nation. These systems can be as relatively "simple" as servers that contain files relating to open criminal investigations, or as complex as databases which allow multiple law enforcement agencies to aggregate, share, and analyze information concerning criminal activity nationwide and internationally. While an exhaustive catalogue and discussion of the computerized systems used by federal law enforcement is not practicable in the context of this brief, a short overview of how those systems are generally used is instructive.[2]

- *Computerized Records of Criminal Investigations*. The vast majority of all written records produced by law enforcement officials are, at some point, stored in digital format on computers. In

[2] FLEOA notes that descriptions of computer systems and databases in this brief necessarily omit law-enforcement-sensitive specifications regarding those systems and databases. Should the Court desire more detail on any of these systems or databases, FLEOA can provide that information to the Court.

addition to ongoing case reports filed by investigators, these files often also include extremely sensitive information, such as the names, addresses, phone numbers and other personal information of victims, suspects, and witnesses.

- *Records Concerning Individuals Whose Identities Require Protection*. Law enforcement maintains records of the identities of a variety of people whose physical safety relies to a great extent on the secrecy of their association with law enforcement. Such individuals include protected witnesses, confidential informants, and undercover officers.

- *Policies and Procedures*. Each law enforcement agency maintains written documentation concerning how it conducts its operations. These records include both generally-applicable policies, such as a description of how a border control agent will typically conduct a search at an international crossing, as well as plans for individual operations, such as how the Secret Service will be deployed during a specific protection detail.

- *Communications Systems*. Computerized hardware and software communications systems used daily by law enforcement officers provide for both traditional written correspondence (email and text messages) and immediate transmission of orders to law enforcement personnel, including agents working in the field.

- *Intelligence Sharing Systems*. Many law enforcement agencies, both local and federal, maintain databases of criminal and intelligence activity which aggregate information gathered

from an array of sources. These systems allow law enforcement agencies to, among other things, identify patterns in crimes from which more effective enforcement techniques may be derived, and to access files created by other agencies which may assist in their investigations. Examples of such systems include the Narcotics and Dangerous Drugs Information System (NADDIS), which is an interface allowing law enforcement agents to access U.S. Drug Enforcement Administration data, and the National Child Victim Identification Program (NCVIP), operated by the Child Exploitation and Obscenity Section of the Department of Justice, which is a database of seized child pornography that is used to identify the abused victims of child pornography.

- *Personnel Information*. Like almost every other entity in the United States that employs individuals, law enforcement agencies also operate computerized systems that contain confidential human resources and payroll records of civilian agency employees and uniformed and non-uniformed law enforcement officers. These records include names, home addresses, personal telephone numbers, Social Security Numbers, names of relatives (and emergency contacts), health records, and bank account direct-deposit, pension and retirement and other benefits records, to name but a few examples. A security breach that results in the exposure of this type of information could result in physical harm, threats, or harassment targeting both law enforcement officers and agency civilian employees. This concern is not unique to law enforcement, although law enforcement officials, like legislators and

member of the judiciary, by virtue of their positions, may be more likely targets of physical threats and other malicious activity than other members of the public should this information be disclosed.[3]

B. Law Enforcement Systems and Databases are Legitimately and Regularly Accessed by a Large Number of Users

The computerized systems used by law enforcement are intended primarily for the use of law enforcement agents, but *many* authorized users have access to these systems. According to the Bureau of Justice Statistics, as of 2016 there were more than 132,000 full-time federal law enforcement officers employed by 83 federal agencies, along with hundreds of thousands of state and local officers.[4] Considering only these officers, however, greatly understates the number of users who have legitimate access to law enforcement systems. In addition to law enforcement officers, federal agencies (and state and local police forces) employ a huge number of civilians in roles such as

---

[3] As the press has noted, a recent report by the Department of Homeland Security warns that personal information including names, email addresses, phone numbers, and home addresses of law enforcement personnel has been posted to social media as part of a malicious "doxing" campaign directed against law enforcement officials. Should that information have been accessed through unauthorized use of law enforcement databases by insiders, the CFAA should be available to prosecute such conduct. *See* Michael Balsamo and Colleen Long, *AP Exclusive: Police Officers' Personal Info Leaked Online*, Associated Press (Jun. 10, 2020), https://apnews.com/23a5e9d316127994ae31ad4813db3f80.

[4] U.S. Dep't of Justice, Office of Justice Programs, Bureau of Justice Statistics, *Federal Law Enforcement Officers, 2016 — Statistical Tables*, NCJ 261992 (Oct. 2019), https://www.bjs.gov/content/pub/pdf/fleo16st.pdf.

crime analysts, dispatchers, forensic technicians, and records management. Beyond that, many agencies necessarily must employ outside contractors to support their activities, including in areas such as data entry and IT technical support which necessitate permissioned access to sensitive law enforcement computer systems and databases. In total, it is reasonable to estimate that substantially more than 1 million individuals have technological access to one or more non-public law enforcement computer system as part of their legitimate job responsibilities. With numbers such as these, the lack of a powerful disincentive to abuse legitimate access or a muscular mechanism to redress abuse poses real peril.

II. THREATS TO LAW ENFORCEMENT DATABASES AND COMPUTER SYSTEMS ARE THREATS TO PUBLIC SAFETY AND TO THE ADMINISTRATION OF JUSTICE

As a result of the nature of the data stored on law enforcement computer systems and the critical role those systems play in law enforcement's routine activities, malicious actors who misuse such confidential information could create significant threats to the safety of individuals and to the integrity of ongoing investigations.

Wholesale access to active, secure investigation files, without the possibility of redress through the CFAA looms as a critical threat over law enforcement's operations. In the most troubling scenario, the targets of investigations could become aware of both the existence of those investigations and the specifics of what law enforcement knows of their activities and how it intends to continue the investigation. This form of knowledge could be used, for example, to destroy evidence, to terminate relationships with exposed

undercover officers, or to flee prior to the execution of a search warrant. More subtly — but perhaps even more insidiously — a corrupt individual with access to investigative files could easily *alter* key facts in those records in a manner that leads officers to misinterpret situations or that introduces a flaw in a search warrant application or even an arrest — and could even undermine confidence in all information in the database.

Moreover, even "closed" files often contain extremely sensitive information concerning the identities of individuals whose physical and/or emotional well-being is dependent on the confidentiality of those files. These dangers include physical threats resulting from criminal organizations becoming aware of the identities of undercover officers, confidential informants, cooperating witnesses or federally-protected witnesses. They also include non-physical dangers to privacy safeguards that the law affords to the identities of certain classes of individuals, including minors and the victims of sexual offenses. That law enforcement databases often act as a historical record of an agency's activities only heightens the threats posed by malfeasance in relation to those systems and databases.

Another example of the danger unregulated insider access poses concerns a law enforcement agency's internal procedures. These procedures can be as seemingly mundane as the processes for checking out an agency-owned vehicle, or as sophisticated as the network security protocols in place to protect the agency's computer systems from outside attacks. The efficacy of these law enforcement "playbooks" are largely dependent on the fact that their contents are unknown to criminals and criminal enterprises. For example, were narcotics traffickers to become aware of the precise scale and capabilities of the Drug

Enforcement Agency to detect smuggling operations, or the manner in which those capabilities are routinely deployed, they could — *and would* — design their operations to avoid detection. Knowledge of computer system vulnerabilities gained by a malevolent insider could also lead to an outsider hacking into a highly sensitive criminal or national security database at will.

Plans for specific operations are another aspect of law enforcement procedures that must be kept confidential. For example, federal agents are often tasked with transporting protected witnesses or protecting members of the executive, legislative and judicial branches during public appearances. An individual who intends to perpetrate an act of violence against a protected individual would obviously be greatly advantaged by advanced knowledge of the identities, locations, and assignments of each agent participating in a protection detail.

These examples are far from exhaustive. Like any other organization with competitors, law enforcement derives benefits from the fact that its adversaries are unaware of its confidential information. In the business context, the ability to keep proprietary information confidential from commercial competitors can afford a financial advantage. But for law enforcement, where the "competitors" are *criminals* and *criminal organizations*, the consequence of having the "playbook" known to the opponent is an undeniable and significant diminution of public safety. In the most egregious scenario, it can mean the difference between life and death.[5]

---

[5] Consider, for example, the case of a disgruntled agency contractor who, because their bill was not paid on time, makes public *all* of the information on a law enforcement operations

III. THE CFAA IS A PROVEN METHOD OF PROTECTING GOVERNMENT SYSTEMS FROM INSIDER THREATS

A. The Threat of Data Theft

That the CFAA may be used to punish outsiders who cause damage to government computers has been well established at least since the Second Circuit's decision in *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991) (upholding the conviction of defendant who released "worm" malware onto the Internet when the worm subsequently caused damage to systems including military computers), *cert. denied*, 502 U.S. 817 (1991). But it is also important to recognize that interpretation of the CFAA as advocated by *Amici* has proven an invaluable tool in combatting cybercrime committed by insiders who target law enforcement computer systems.

An examination of several cases in which a computer operator was granted access permission to a system and was then prosecuted for malicious acts committed outside the scope of that access, is instructive:

- *Abusing Civilian Access to Provide Details of Ongoing Investigations to Criminals.* In 2009, a civilian employee working as a data entry clerk for a contractor was tasked with entering data into the NADDIS database. While having clear permission to be on the system, the clerk was

---

database to which they have access. Or an IT consultant with technological access to a government personnel database who posts on the Internet *all* of the personal information of *all* of the civilian and non-civilian employees of a given law enforcement agency because of disdain for that particular agency — or for law enforcement generally. In these situations, real harm may befall *numerous* victims.

prohibited, as a matter of policy, from using NADDIS for any purpose other than entering records supplied by law enforcement agents. The policy also prohibited the clerk from querying NADDIS for any other purpose, and the clerk was, by written agreement, expressly warned that the disclosure of NADDIS files could endanger DEA investigations. As a result, she was not permitted to communicate any information found in NADDIS. In flagrant violation of these policies, the clerk subsequently used her access to NADDIS to obtain information concerning the DEA's investigation into two individuals, including her romantic partner, and divulged details concerning the investigation to those individuals.[6] The details included that law enforcement had placed a GPS tracker on a co-conspirator's car. As a result of the clerk's activities, law enforcement was forced to execute search warrants earlier than anticipated and, likely as a result of being "tipped off," only one other member of the drug organization was arrested and charged. The clerk was indicted and pleaded guilty to conspiracy stemming from her violations of the CFAA.[7]

- *Local Employee Using Federal Access to Commit Identity Theft.* While the CFAA is a federal statute, it has been effective at the state and

---

[6] Indictment, *United States v. Perry*, No. 09-cr-0090 (D. Md. Feb. 25, 2009).

[7] U.S. Attorney's Office for the District of Maryland, *DEA Contractor Pleads Guilty to Illegally Accessing Government Database*, U.S. Department of Justice (Oct. 20, 2009), https://www.justice.gov/archive/usao/md/news/archive/DeaContractorPleadsGuiltytoIllegallyAccessingGovernmentDatabase.html.

local level as well. In a recent example, a civilian employee of the Tampa Police Department was tasked with taking down reports from citizens and entering them into various law enforcement databases. To accomplish this task, she was provided access to, among other databases, the National Crime Information Center (NCIC) computerized index: a system maintained by the Federal Bureau of Investigation for the purpose of assisting law enforcement agents to perform their official duties. The civilian employee was restricted from using the NCIC for any purpose other than the performance of her authorized duties. In clear violation of these policies, as part of an identity theft conspiracy, the civilian employee accessed the personal information of individuals in the NCIC database and provided that information to co-conspirators who used it to file fraudulent federal income tax returns in order to obtain fraudulent tax refunds from the government. The civilian *had* authorized access; however, she misused it. Consequently, the employee was indicted in 2015 on a number of federal charges, including a violation of the CFAA.[8]

- *Theft of Military Intelligence.* In 2010, U.S. Army Private Chelsea Manning (known then as Bradley Manning) downloaded a large trove of

[8] Indictment, *United States v. Bright*, No. 15-cr-00366 (M.D. Fla. Sep. 9, 2015); *see also* U.S. Attorney's Office for the Middle District of Florida, *Former Police Department Employee Indicted for Tax Fraud, Computer Intrusion, and Identity Theft*, U.S. Department of Justice (Sept. 15, 2015), https://www.justice.gov/usao-mdfl/pr/former-police-department-employee-indicted-tax-fraud-computer-intrusion-and-identity.

sensitive military intelligence documents from a classified database and transmitted them to WikiLeaks founder Julian Assange, who published them online. Private Manning's Top-Secret rating lawfully permitted access to the database. At trial, in addition to espionage charges, Manning was convicted of violating the CFAA.[9]

B. The Threat of Data Manipulation

Another particularly insidious manner in which authorized users of law enforcement computer systems have interfered with officers' duties is through the alteration or insertion of false records into official records. Individuals with access to law enforcement's electronic systems can instruct officers to respond to non-existent threats, thus diverting them from actual crime scenes. Insiders who manipulate records can also remove critical details from investigative records which may stop law enforcement from effectively pursuing a case, while manipulation of historical records can make criminal history invisible to background checks. Subtle alterations in intelligence databases can also conceal the identities or activities of those acting against U.S. interests in the espionage and terrorism realms.

---

[9] On appeal to the U.S. Army Criminal Court of Appeals, Manning challenged the scope of the CFAA, arguing that the statute was misapplied in light of the fact that access to the database was "authorized." The appeals court recognized the circuit split in the civilian courts on this issue and affirmed the conviction based on a reading of the statute advocated by FLEOA. *United States v. Manning*, 78 M.J. 501, 510-11 (U.S. Army Ct. Crim. App. 2018) (noting circuit split between First, Fifth, Seventh, and Eleventh Circuits and Second, Fourth, and Ninth Circuits).

At first glance, it would seem as though the various CFAA subsections which prohibit conduct based on a defendant's exceeding his access to a computer would govern these examples, as subsection (e)(6)'s definition encompasses the alteration of information that the "accesser" is "not entitled" to "alter." Clearly, a law enforcement employee is not entitled to alter or falsify agency records. However, since "entitled" is just as undefined in the CFAA as is "without authorization," we confront the same conundrum concerning the distinction between technological measures and communicated permissions. What would stop, for example, a records clerk who deletes a law enforcement file from claiming that he was "*entitled*" to do so purely on the basis of his technical permission to access to those records as part of his legitimate job duties?

This concern is not merely hypothetical. Examples of law enforcement "insiders" who have manipulated records for criminal purposes through their legitimate technical access include:

- *Attempts to Corrupt Law Enforcement Databases.* In 2010, a former data analyst working from the Transportation Security Administration's Colorado Springs Operations Center (CSOC), tasked with updating the TSA's servers with data received from the federal Terrorist Screening Database and the U.S. Marshal's Service Warrant Information Network, transmitted malicious code to the TSA's system in an intentional attempt to corrupt the CSOC's systems and interfere with those systems' ability to be used to screen air passengers. The data

analyst was indicted and pleaded guilty to charges under the CFAA.[10]

- *Falsification of Records to Enable Identity Theft.* In 2011, a contractor who worked as a records custodian at U.S. Citizenship and Immigration services pleaded guilty to violating the CFAA in connection with a scheme in which he assisted illegal aliens in obtaining U.S. passports by *deleting* the names, birth dates and other personal information of naturalized citizens in a secure database and *substituting* them with the personal information of illegal immigrants. Subsequent searches for the illegal immigrants by government officials would then indicate that the individuals were citizens entitled to passports.[11]

- *Falsification of Records to Cause Detention of An Innocent Person.* In 2018, a former U.S. Border Patrol Agent pleaded guilty to creating and entering into TECS (a database used by officers to assist in screening at border crossing) a false law enforcement alert claiming a man with no criminal history was frequently armed with a firearm and known to be linked to the narcotics trade, resulting in that man's being detained multiple times at border crossings. The former agent had created the false alert in

---

[10] Indictment, *United States v. Duchak*, No. 10-cr-00131 (D. Colo. Mar. 9, 2010); *see also* U.S. Attorney's Office for the District of Colorado, *Colorado Springs Man Indicted for Attempting to Corrupt TSA Computer Database*, U.S. Department of Justice (Mar. 10, 2010), https://www.justice.gov/archive/usao/co/news/2010/March10/3_10_10.html.

[11] Information, *United States v. Quidilla*, No. 11-cr-00617 (S.D. Cal., Feb. 17, 2011), Dkt. No. 14.

an effort to coerce the victim into dropping criminal sex abuse charges against the agent's brother-in-law.[12]

All of the above are instances which would fall outside the purview of the CFAA were Petitioner's view of the statute be adopted.

IV. A PURELY "OUTSIDE HACKER" INTERPRETATION OF THE CFAA WOULD LIMIT ITS UTILITY AND IMPOSE SUBSTANTIAL COSTS ON ITS USE

Should the CFAA only prohibit the conduct of those who access systems to which they are *technologically* denied access, rather than also taking into account procedural and policy prohibitions, the only recourse for any entity — law enforcement or otherwise — to protect its systems will be to strictly limit technical authorization for *each* individual who uses those systems. This authorization will necessarily be limited to only the *absolute minimum* required to accomplish their job responsibilities. This is not practical. It also makes no sense.

For multiple reasons, imposing strict user-based limitations on access to specific files and systems is an expensive, time-consuming, and inefficient process.

---

[12] Complaint, *United States v Figeroa et al.*, No. 15-cr-02818 (S.D. Cal. Oct. 7, 2015) (defendant Duran in this case was charged with a violation of Title 18, United States Code, section 1519 (Destruction, alteration, or falsification of records in Federal investigation) rather than of the CFAA); *see also* U.S. Attorney's Office for the Southern District of California, *Former U.S. Border Patrol Supervisor Pleads Guilty, Admits to Violating Civil Rights of Legal Border Crosser*, U.S. Department of Justice (Aug. 16, 2018), https://www.justice.gov/usao-sdca/pr/former-us-border-patrol-supervisor-pleads-guilty-admits-violating-civil-rights-legal.

First, file permissions would have to be set on a file-by-file basis, rather than system or database-wide. *Second*, each user would have to be granted or denied access to each file on an individual, rather than group-based basis. And *third*, the administrator of each system would be deluged with requests for exceptions to the access-control policy so that frontline workers could simply do their jobs.

In the context of law enforcement, this would require, for example, only allowing an agent access to the specific case files for the investigations to which he or she is assigned at that very moment. Database overseers would then be inundated with requests from agents to grant one-time access to other files or systems. The alternative — allowing agents access to files not directly related to their day-to-day tasks — would expose data to misuse, alteration, or destruction without the possibility of criminal recourse or even civil sanction under the CFAA.[13] Additionally, as law enforcement supervisors would in many cases continue to have unfettered access to the databases in use by their subordinates, supervisors would have carte blanche to access, manipulate or delete data in any manner they chose.

Applying such a "hacker-only" CFAA regime to the administration of the NADDIS database (mentioned

---

[13] Although some wrongdoing — for example, exfiltration of classified information by a corrupt insider from an intelligence community database — might be covered under other federal criminal statutes, that may not always necessarily be so. Moreover, even in cases where other crimes could theoretically apply to clearly blameworthy data destruction, theft, or misuse by an insider, the loss of the clear and straightforward provisions of the CFAA (as understood by FLEOA) would remove a valuable tool available to prosecutors to redress these wrongs.

above) is instructive. NADDIS is currently protected from unauthorized access by administrative, technical, and physical means and all authorized users acknowledge in writing that they may not disseminate the information contained on the system. Through these safeguards, access to NADDIS is restricted only to those who use the system for specific assigned tasks. These authorized users include DEA agents as well as civilian employees who, for example, enter data into the system. Technical access can, however, be granted to "groups" of users by allowing, for example, all DEA employees who are agents and supervisory agents permission to view certain records within the database.

If Petitioner's proposed interpretation of the CFAA is adopted, to ensure that data contained within NADDIS continues to be maximally protected, access to NADDIS would have to be further restricted by taking such steps as *eliminating* group-based authorizations and restricting each *individual* agent to access records concerning the cases on which that individual agent is currently working. Under this approach, granting permissions to access NADDIS potentially changes from a simple, role-based and largely one-time authorization, to one in which every document or electronic record entered into the database would need specific, unique access criteria assigned to it. In addition, should a DEA agent wish to view NADDIS entries for other matters (for example, to see if any other investigations have involved similar factual circumstances), the agent would have to request permission to access those records — a cumbersome process which would delay access to data during a time-sensitive investigation.

It is this latter issue which reveals the subtler, but more critical, problem with strict file-based access

control mechanisms: They remove the ability of computerized systems to be used for intelligence and information *collaboration and sharing*, thus defeating the very purpose for which many law enforcement databases are designed. NADDIS, along with numerous other law enforcement databases, exist primarily to allow law enforcement the benefit of shared intelligence and iterative analysis of information which has been gathered by agents and officers nationwide and even internationally. These officers are then able to leverage this aggregated knowledge to inform their investigations and enforcement activities.

If the CFAA is interpreted not to criminalize misuse of data to which technical access has been granted, law enforcement will be deprived of a powerful tool — in some cases the only tool — to deter and punish unauthorized misuse of vital criminal intelligence systems and databases.

CONCLUSION

Given the critical nature of the computerized systems used by federal law enforcement agencies on a daily basis and the threats to those systems both from insiders and outsiders, a narrow reading of the CFAA limited only to outsider "hackers" would allow acts which are commonly and reasonably perceived as serious cybercrimes to fall outside the scope of the statute. It is therefore essential to the public safety mission of federal law enforcement agents that the Court accord the term "unauthorized access" as it is used in the CFAA, according to its plain meaning so as to protect non-public, sensitive data from malicious misuse or vandalism from both external *and internal* wrongdoers.

Respectfully submitted,

JOSEPH V. DEMARCO
Counsel of Record
DAVID M. HIRSCHBERG
ERIC SEIDEL
BRIAN A. FOX
DEVORE & DEMARCO LLP
99 Park Avenue, Suite 1100
New York, NY 10016
(212) 922-9499
(917) 576-2369
jvd@devoredemarco.com

Counsel for Amicus Curiae

August 31, 2020