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 KAREN HEART AND ANTHONY VOLINI OF CIPLIT AS AMICI CURIAE IN SUPPORT OF RESPONDENT

Karen Heart
*Counsel of Record*
Anthony Volini
CENTER FOR
INTELLECTUAL PROPERTY
LAW & INFORMATION
TECHNOLOGY
DePaul College of Law
25 E. Jackson Blvd.
Chicago, IL 60604
(312)362-1469
kheart@depaul.edu

**TABLE OF CONTENTS**

## TABLE OF CITED AUTHORITIES

**Cases** **Pages**

**Statutes** **Pages**

## INTEREST OF THE AMICUS CURIAE

DePaul's Center for Intellectual Property Law & Information Technology (CIPLIT®) was established to promote research and concentrated study of intellectual property and information technology law, broadly defined. We seek to develop IP professionals of the highest caliber through an all-inclusive learning experience that combines outstanding classroom education, innovative scholarship, first-class training in lawyering skills, career counseling and an unparalleled range of extracurricular activities.

As faculty of CIPLIT, we submit[1] this brief amicus curiae because of the urgent need to harmonize the rule of law with computer technology. We teach courses on cybersecurity and data privacy and, therefore, are intimately familiar with the practices and procedures necessary for maintaining proper computer security. Accordingly, we believe that it is essential that any decision concerning the reach of the CFAA be grounded in the practicalities of data protection. Our argument clearly distinguishes malicious behavior that the CFAA aims to prohibit from innocuous behavior that does not infringe on possessory interests.

---

[1] No counsel for a party authored this brief in whole or in part. No person other than amici curiae have made a monetary contribution to its preparation or submission. The parties have consented to the filing of this brief.

## SUMMARY OF THE ARGUMENT

The Computer Fraud and Abuse Act (CFAA) was designed to protect against misuse of data stored in computers. Indeed, the CFAA is the primary federal law designed to protect employers from employee theft by misuse of computers. By affirming Petitioner's conviction and overruling contrary holdings, employees could be held accountable for abuses of information for which the employer holds a superior possessory interest.

Moreover, the language of the CFAA does not support prosecutions for ordinary behaviors, such as checking one's Facebook account while using a computer at work. The crux of the argument by the Petitioner and various amici curiae is that the CFAA can be used to overreach in such circumstances. This concern is unfounded because customary activities, such an employee's visit to Facebook, does not infringe any possessory interest of the employer that is required for conviction under section (a)(2) of the CFAA.

## ARGUMENT

### I. THE CFAA PROTECTS EMPLOYERS FROM TREACHEROUS EMPLOYEES WHO STEAL EMPLOYER OWNED OR CONTROLLED PROPERTY, TYPICALLY ELECTRONIC INFORMATION.

Prior to enactment of the CFAA, various precedents supported the principle that stealing employer owned or controlled property supports a criminal charge notwithstanding the generally contractual nature of the employment relationship. This principle includes theft of employer money or misuse of employer assets for personal benefit so long as the misuse is clearly not authorized by the employer. In the context of the CFAA, the employer property is typically electronic information owned or controlled by the employer. However, pre-CFAA cases involving traditional property, such as money or physical assets, provide precedent on the general principle of misuse of employer property supporting a criminal charge. A core issue is whether the employee has exceeded the scope of his employer's consent with regard to use of employer entrusted money or other assets. A very clear example of this principle occurred in *People v. Schueneman*, 320 Ill. 127, 150 N.E. 664 (1926). Schueneman, an employee bookkeeper, was authorized to deposit his employer's funds into the bank but, on one occasion, skimmed money from employer deposits. The Illinois Supreme Court held that the defendant's taking of the funds was beyond the authority given by the employer and, therefore, upheld the conviction for theft.

The same principle was applied recently in *People v. Oglesby*, 2016 IL App (1st) 141477, 69 N.E.3d 328 (1st Dist. 2016). Oglesby was the deputy chief of staff for the president of the Cook County board and used her authority to issue contracts with private entities that she owned. Despite her authority to spend employer funds, the appellate court upheld her conviction for theft because she accepted payment, pursuant to a contract, but never rendered the contracted for services.

An employee can also steal from his employer by misusing employer assets entrusted to him for work purposes. In *People v. Hajostek*, 49 Ill. App. 3d 148, 149, 363 N.E.2d 1208, 7 Ill. Dec. 46 (3rd Dist. 1977), the defendant used his government work truck and gravel for personal profit; specifically, he used the employer's truck to deliver and sell government owned gravel to a private party. Although the employee was authorized to use the truck to haul gravel for a township, his use of those assets for self-profit were very clearly outside the scope of his employer's consent, and thus his theft conviction was affirmed.

This principle was applied to burglary in *State v. Sawko*, 624 So.2d 751 (Fla. Dist. Ct. App. 1993). The defendant was a maintenance worker employed by a landlord. As might be expected, the employer landlord gave its employee maintenance worker a physical master key to access all of the employer's tenant occupied units. Nonetheless, the appellate court in Florida held that the maintenance worker could be found guilty of burglary if he entered units for an

unauthorized purpose, such as to steal tenant owned property.

Hence, the question of consent has long constituted a legitimate element in the prosecution of employees for property crimes. Because due process demands that proof of each element meet the reasonable doubt standard, circumstances that reveal ambiguity fail to support a conviction. For example, in *People v. Lewandowski*, 43 Ill. App. 3d 800, 357 N.E.2d 647, 2 Ill. Dec. 480 (2nd Dist. 1976), a college purchasing agent, along with his codefendant, bought surplus federal government property to sell to a third party and then return the proceeds to the college. When the codefendant kept some of the proceeds, both the defendant and codefendant were charged with theft. However, the appellate court reversed the conviction because there was insufficient evidence to prove that the federal government had not consented to the reselling of its surplus property.

There is no reason why traditional notions of consent to use of property should not be applied to criminal prosecutions under the CFAA, which may be viewed as tantamount to a state law theft charge. Indeed, the CFAA is the primary federal law designed to protect employers from employee theft by misuse of computers. In *WEC Carolina Energy Solutions v. Miller*, 687 F.3d 199; 2012 U.S. App. LEXIS 15441 (4th Cir. 2012), the defendants obtained confidential information and trade secrets given their authorized access as employees of WEC. Subsequently, the defendants used the information to help one of WEC's competitors obtain a contract from a company that

had been a potential customer of WEC. WEC sued, alleging violation of the CFAA, but the district court dismissed the claim and the Fourth Circuit affirmed, holding that the CFAA was not unambiguous as to such liability. Stealing an employer's trade secrets for the employee's own benefit is quite clearly outside the scope of the employer's consent, even when the employee is granted access to the secrets maintained on a computer as part of that employee's duties. Holding one accountable for stealing employer owned or controlled information by misuse of authorized computer credentials is clearly within the purview of Congress; this Court must overrule the decision in the *WEC* case by affirming Petitioner's conviction.

In *United States v. Valle*, 807 F.3d 508, 2015 U.S. App. LEXIS 21028 (2nd Cir. 2015), the defendant was a New York City police officer. Pursuant to his employment, Valle was provided access to databases that contained sensitive personal information about a variety of individuals. NYPD's policy was that the databases were to be accessed only for official police business. In May of 2012, Valle accessed these databases in order to gain information about a woman whom he fantasized about kidnapping and murdering. Valle admitted accessing the database for his own personal purposes and was convicted of violating the CFAA, but the Second Circuit reversed the conviction on the basis that the intent of the CFAA was unclear. By affirming Petitioner's conviction and overruling the decision by the 2nd Circuit, people such as Valle could be held accountable for such outrageous misuses of their employer's databases, especially considering the strong governmental interest in

protecting the privacy of civilians. Thus, this Court must allow the government to pursue a criminal charge under section (a)(2) of the CFAA, particularly where an employee's violation of an employer rule regarding use of data is especially egregious, such as sharing the information with a third party for personal gain, as in this case, in order to vindicate the goal of Congress to prevent such illicit market activity. In another situation, section (a)(2) could be violated where the defendant views classified governmental secrets without an authorized purpose.

## II. THE CFAA IS A MODERN TOOL TO CRIMINALIZE EMPLOYEE THEFT OF EMPLOYER OWNED OR CONTROLLED INFORMATION MUCH LIKE ITS PRECURSORS, THE MAIL AND WIRE FRAUD ACTS.

Computers have replaced a large volume of data transmission that used to be handled by the U.S. Postal Service and telephone calls. The federal mail fraud statute, 18 U.S.C. § 1341, prohibits the use of the U.S. mails to execute a fraudulent scheme. Similarly, 18 U.S.C. § 1343, the wire fraud statute, prohibits the use of electronic communication to execute a fraudulent scheme. Thus, to the extent that it prohibits the use of computers to execute employee misuse of employer owned or controlled information, the CFAA can be loosely viewed as the modern equivalent of the mail and wire fraud statutes. It follows that application of the CFAA to such situations is equally permissible under the

Constitution as the application of the federal mail and wire fraud statutes.

In *Carpenter v. United States*, 484 U.S. 19 (1987), this Court addressed the question of whether conspiracy to trade on a newspaper's confidential information was within the reach of federal mail and wire fraud statutes. Carpenter was convicted because he was found to have aided and abetted others in a conspiracy to commit mail and wire fraud. Winans, a reporter for the Wall Street Journal, worked on a daily column that gave positive and negative advice pertaining to stock information. In gathering the content for these articles, Winans interviewed and received confidential information that, under the policies of the Wall Street Journal, belonged to the Journal prior to publication. Nonetheless, Winans entered into a conspiracy with several individuals who worked at a New York brokerage firm and Carpenter to make profitable trades of securities based on the yet to be published information. This Court found that the confidential information was generated by the Wall Street Journal in its function as a business and, thus, that the Journal had the right to decide how the information would be used prior to it being released to the public. This Court ruled that fraud, as used in the mail and wire fraud statutes, included embezzlement, "which is 'the fraudulent appropriation to one's own use of the money or goods entrusted to one's care by another.'" *Carpenter* at p. 27, citing *Grin v. Shine*, 187 U.S. 181, 189 (1902). Accordingly, this Court affirmed Carpenter's convictions for mail and wire fraud.

As in *Carpenter*, the Petitioner fraudulently appropriated data for his own use that had been entrusted to his care by his employer, the Cumming, Georgia, Police Department. Had Petitioner placed the data in the mails or communicated it electronically, he would have been found guilty of mail or wire fraud. Because he obtained the data by exceeding his authorized access, however, he violated the CFAA. The fact that his conviction is based partly on the policy of his employer regarding use of law enforcement data does not differ from the fact that the conviction of Carpenter was, likewise, based partly on the policy of the Wall Street Journal regarding use of its confidential data. Like the mail and wire fraud statutes, the Computer Fraud And Abuse Act, according to the second word in its name, was enacted, in part, to prohibit the use of a computer as the instrumentality to execute fraudulent activity.

## III. ACTIVITY THAT DOES NOT INVOLVE UNAUTHORIZED ACCESS OF DATA OWNED OR CONTROLLED BY A VICTIM IS OUTSIDE THE SCOPE OF SECTION (a)(2) OF THE CFAA.

It is well settled law that authorization to access and use property is predicated on consent of the party having the greater possessory interest, typically the owner. Application of this principle to property interests in computers is exemplified in *People v. Janisch*, 2012 IL App (5th) 100150, 966 N.E.2d 1034 (Ill. App. Ct. 2012). In *Janisch*, the defendant was charged with violating an Illinois statute, the

Computer Crime Prevention Law, that is analogous to the CFAA. In particular, the defendant was convicted of accessing the email account of her ex-husband without authorization. On appeal, the defendant argued that there was insufficient evidence because the State did not offer evidence that she physically accessed her ex-husband's computer or that she accessed MSN's computer, which maintained the emails, without consent. Citing the language of the Illinois law, the court held that her ex-husband held a possessory interest in MSN's computer and, therefore, could control who was authorized to access his email account on it. In short, the public, including the defendant, was permitted to access MSN's computer in order to access their own email accounts maintained by MSN, but the defendant exceeded her authority by accessing her ex-husband's email account on that computer without his consent. This holding fits squarely within the long, venerable history of jurisprudence considering consent to access property as an element of a criminal charge. Neither the Petitioner nor the other amici curiae have advanced a reason to abandon this precedent.

Given this rule of law regarding possessory interest, there is no reason to fear that ordinary activities, such as accessing one's account on Facebook to send a message while using a work computer, would qualify for prosecution under the CFAA. Because the user owns her/his data and, therefore, has the lawful right to access her/his data maintained on Facebook's computers, as well as permission from Facebook to send a message to another user, the fact that the access occurs through a computer owned by one's

employer makes no difference to the issue of authorized access of Facebook's computers. Alarmist fears that affirming Petitioner's conviction would give rise to criminal liability for such mundane acts are unfounded.

The crux of the argument by the Petitioner and various amici curiae is that the CFAA can be used to overreach in such circumstances. This concern arises primarily from two cases, *United States v. Drew* and *United States v. Manning*. A review of these cases, however, reveals that the concern arose from judicial error rather than the language or intent of the CFAA.

In 2006, Lori Drew participated in a scheme with others to post a fake profile on the MySpace website, in direct contravention of MySpace's terms of use. Drew and the others posted a caustic message to another MySpace user whom they knew in real life; the message stated that the world would be better off without this other user, who was a young teenage girl. Later that day, the girl committed suicide. The US Attorney's office prosecuted Drew for criminal violations of the CFAA and a jury found Drew guilty of violating section (a)(2) of the CFAA. Subsequently, the trial judge granted Drew's motion to set aside the verdict on the basis that the reliance on provision (a)(2) to prosecute this offense was impermissibly vague. *United States v. Drew*, 259 F.R.D. 449, 2009 U.S. Dist. LEXIS 85780 (C.D. Cal. 2009). Specifically, the court held that using the CFAA to prosecute one for violating a term of use prohibiting the posting of fake profiles was constitutionally vague. While the final result of dismissing the case was correct, the fact

that the trial judge let the matter proceed to jury deliberation and verdict puts the public on notice that computer users may be subjected to the jeopardy of criminal proceedings before an improper prosecution under the CFAA is halted. This error has struck terror into the hearts of users everywhere and given impetus to the amici curiae appearing before this Court.

This Court can best serve justice by taking care to explain the error of such misguided enforcement efforts. Notably, the general principle that a mere violation of a term of use cannot serve as the basis for a prosecution under the CFAA was reaffirmed in *Facebook v. Power Ventures*, 844 F.3d 1058, 1066 (9th Cir. 2016). Therefore, the Court should rule that violating an alleged victim's terms of use does not rise to the level of a section (a)(2) violation where no information owned or controlled by the victim was obtained or altered. Applying this reasoning to *Drew* would best explain the error therein while affirming the dismissal of the charge. Affirming the reasoning in *Facebook v. Power Ventures* and supplementing with the foregoing reasoning will provide resolute guidance against spurious threats to prosecute those who violate terms of use, even unintentionally. More importantly, this Court must clarify that any prosecution under section (a)(2) of the CFAA rests on the question of consent and that a term of service would be applicable only to the extent that it clearly established the possessory interests of the parties to the contract as to computer information.

The more troubling case is *United States v. Manning*, 78 M.J. 501, 2018 CCA LEXIS 264, 2018

WL 2437948 (A. Ct. Crim. App. 2018), which, admittedly, has less precedential value because it was a court martial. Manning was an Army intelligence analyst who downloaded classified documents and gave them to Wikileaks, which published them. Manning was prosecuted in a court martial, in part, for violating section (a)(1) of the CFAA, relating to transmitting classified data by accessing it in excess of authority. During the proceedings, it was revealed that Manning used a prohibited software program that automated the downloading of the classified data, rather than accessing the data manually as was required by Department of Defense policy. The court found that Manning had exceeded authority under the CFAA by using the prohibited software; the military court of appeals affirmed. Notably, the Court of Appeals mused that had Manning downloaded the data manually, "this would present a different issue." *Manning* at 512. The CFAA, however, mentions neither; nor does it mention anything about the manner that data is accessed. Indeed, the definition of accessing data in excess of authority is simply a question of whether the person is entitled to access the data. Section (e)(6) states that "the term '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." Because Manning was not entitled to obtain information in the computer for purposes other than assigned military duties, such as publishing it on WikiLeaks, Manning exceeded authorized access of the computer; whether Manning accessed the information manually or by use of

automated software was irrelevant. Congress could have added language about the manner of access, such as software that automates downloading, but did not. Hence, the military courts made an erroneous holding that the manner of access was the determining factor. This Court must not let the erroneous reasoning in the *Manning* opinion stand.

By applying the language of the CFAA precisely, it becomes evident that the CFAA does not support the criminalization of any behavior prohibited simply by a terms of use agreement. In particular, the CFAA does not prohibit the intentional creation of false user profiles. In the *Drew* case, the defendant created the profile and stored it on the MySpace computer. Because Drew had a valid account that authorized her to create a profile and store the data, she did not access data stored on MySpace's computer without authorization. More importantly, because MySpace had given her an account that was designed specifically to permit her to store a profile on the MySpace computer, Drew did not exceed her authority by storing the fake profile. Hence, section (a)(2) did not prohibit Drew's conduct. Assuming arguendo that Drew understood that the MySpace terms of use prohibited the posting of fake profiles, Drew falsely agreed to MySpace's terms of use in order to gain access to their computer. In other words, she committed fraud against MySpace in order to obtain authorization. The CFAA prohibits precisely such conduct but under section (a)(4). Nonetheless, section (a)(4) also provides that the fraud must be for a purpose other than to access the computer unless the value of the use exceeds $5000 in one year.

Accordingly, that section did not prohibit the fraud perpetrated by Drew. Hence, investigative journalists, security researchers, and others who must rely on the use of fake account profiles in order to conduct bona fide research would similarly not be subject to either section (a)(2) or (a)(4) of the CFAA for doing so.

Moreover, section (a)(2) of the CFAA makes no mention of software and certainly does not prohibit the use of scraping techniques. As explained earlier, the CFAA makes no mention of the manner of access. Instead, section (e)(6) clarifies that exceeding authorized access is based solely on the question of whether one is entitled to obtain data. Nonetheless, as conceded in the amicus curiae brief of the ACM, section (a)(5) of the CFAA does prohibit scraping behaviors, as well as any other conduct involving access, that is so excessive that it causes significant damage.

A careful examination of the language of the CFAA reveals that it was crafted to balance competing interests. Indeed, the use by whistleblowers of the afore-mentioned techniques does not give rise to liability under the CFAA. However, the publication of confidential data by whistleblowers can be prohibited by the CFAA. Divulging private data-- even to journalists, may be considered criminal conduct under certain circumstances, such as divulging classified governmental information or trade secrets. Absent such circumstances however, a business may not try to hide evidence of a crime or other violations of the law by way of restrictive computer use policies. Only

a use policy that may be validly enforced can serve as the basis for a prosecution under the CFAA.

The complaint of the amici curiae that computer security researchers have been threatened with prosecution under the CFAA for their activities is, sadly, true. While businesses and security researchers should work together more amicably, the CFAA does not strip businesses of their lawful right to govern their affairs, even when it comes to matters of computer security. In particular, businesses have the right to refuse simulated attacks perpetrated against them by security researchers. If this Court ruled that security researchers can poke and prod the computers of any business under a judicially-created "fair use" doctrine, which is not envisioned by the CFAA, then anyone could penetrate the computer systems of businesses under the guise of security research. It takes little imagination to envision unscrupulous business people hiring so-called security experts to undermine the operations of their competitors. The CFAA prohibits such nefarious practices, and there is no legal reason to thwart the intent of Congress. Nevertheless, computer researchers are well within their rights under the CFAA to conduct security research so long as it does not damage computers or access data that they are not entitled to obtain. Along these lines, various non-invasive scanning techniques are permissible where the scanning is looking for network information viewable to the public because viewing public data does not require authorization. However, a scanning technique followed by some form of penetration into an organization's network would support a section (a)(2) violation where the

perpetrator is accessing victim owned or controlled information that is not publicly visible. Anyone can stand on the street and observe that a building has windows that are open but crawling through one without authorization would constitute a crime.

## CONCLUSION

This Court should affirm the opinion of the 11th Circuit and hold that section (a)(2) of the CFAA can be violated when an employee violates the possessory interest of the employer by accessing data in excess of authority.

Respectfully submitted,

Karen Heart
*Counsel of Record*
Anthony Volini
CENTER FOR
INTELLECTUAL PROPERTY
LAW & INFORMATION
TECHNOLOGY
DePaul College of Law
25 E. Jackson Blvd.
Chicago, IL 60604
(312)362-1469
kheart@depaul.edu

Date: September 2, 2020