No. _____

In The
Supreme Court of the United States

CHARLES DANIEL MAYE,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For A Writ Of Certiorari To The Eleventh Circuit Court Of Appeals

PETITION FOR WRIT OF CERTIORARI

KENT & MCFARLAND,
Attorneys at Law
WILLIAM MALLORY KENT
24 North Market Street,
Suite 300
Jacksonville, Florida 32202
(904) 398-8000 Telephone
(904) 348-3124 Fax
kent@williamkent.com Email
Counsel for Petitioner Maye

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

QUESTION PRESENTED

Whether "exceeds authorized access" in the Computer Fraud Abuse Act ("CFAA") is limited to violations of restrictions on access to information, and not restrictions on its use.

LIST OF PARTIES

Charles D. Maye, Petitioner

United States of America, Respondent

STATEMENT OF RELATED CASES

- *United States of America v. Charles Daniel Maye*, No. 8:04-cr-00321-JSM-EAJ, U.S. District Court, Middle District of Florida, Tampa Division, judgment entered July 24, 2006;
- *Charles Daniel Maye v. United States of America*, No. 8:07-cv-653, U.S. District Court, Middle District of Florida, Tampa Division (2255 withdrawn by Maye), Judgment entered N/A;
- *Charles Daniel Maye v. United States of America*, No. 8:07-cv-1258-T-30EAJ, U.S. District Court, Middle District of Florida, Tampa Division (2255) Opinion entered July 21, 2008;
- *Charles Daniel Maye v. United States of America*, No. 08A460, United States Supreme Court, application for a certificate of appealability denied January 26, 2009;
- *Charles Daniel Maye v. United States of America*, No. 10-11627, U.S. Court of Appeals, Eleventh Circuit, order denying leave to file successive motion to vacate entered May 3, 2010;

STATEMENT OF RELATED CASES – Continued

- *Charles Daniel Maye v. United States of America*, No. 8:10-cv-02327-JSM-TBM, U.S. District Court, Middle District of Florida, Tampa Division (2255), order denying leave to file successive motion to vacate entered April 27, 2012;
- *Charles Daniel Maye v. United States of America*, No. 11-11022, U.S. Court of Appeals, Eleventh Circuit, order denying certificate of appealability entered April 27, 2011;
- *Charles Daniel Maye v. Warden*, No. 2:11-cv-00059-LGW-JEG, U.S. District Court, Southern District of Georgia, Brunswick Division, judgment entered June 23, 2011;
- *Charles Daniel Maye v. Warden*, No. 11-14020, U.S. Court of Appeals, Eleventh Circuit, judgment entered February 28, 2012;
- *Charles Daniel Maye v. United States of America*, No. 12-11782, U.S. Court of Appeals, Eleventh Circuit, order denying leave to file successive motion to vacate entered April 25, 2012;
- *Charles Daniel Maye v. United States of America*, No. 12-270, United States Supreme Court, petition for writ of certiorari denied January 22, 2013;
- *Charles Daniel Maye v. United States of America*, No. 12-14819, U.S. Court of Appeals, Eleventh Circuit, order denying certificate of appealability March 20, 2013;

STATEMENT OF RELATED CASES – Continued

- *Charles Daniel Maye v. United States of America*, No. 8:13-cv-3104, U.S. District Court, Middle District of Florida, Tampa Division, order denying leave to file successive motion to vacate entered January 9, 2014;
- *Charles Daniel Maye v. United States of America*, No. 14-12595, U.S. Court of Appeals, Eleventh Circuit, order denying leave to file successive motion to vacate entered July 10, 2014;
- *Charles Daniel Maye v. United States of America*, No. 14-15531, U.S. Court of Appeals, Eleventh Circuit, order denying certificate of appealability entered March 12, 2015;
- *Charles Daniel Maye v. United States of America*, No. 14-14059, U.S. Court of Appeals, Eleventh Circuit, order denying certificate of appealability entered September 1, 2015;
- *Charles Daniel Maye v. United States of America*, No. 8:17-cv-01314-VMC-MAP, U.S. District Court, Middle District of Florida, Tampa Division, order denying petition for writ of coram nobis entered February 16, 2018;
- *Charles Daniel Maye v. United States of America*, No. 18-13069, U.S. Court of Appeals, Eleventh Circuit, judgment entered April 25, 2019

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

In The
Supreme Court of the United States

CHARLES DANIEL MAYE,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For A Writ Of Certiorari To The Eleventh Circuit Court Of Appeals

PETITION FOR WRIT OF CERTIORARI

The Petitioner, Charles D. Maye, respectfully prays that a writ of certiorari issue to review the order of the United States Court of Appeals for the Eleventh Circuit, entered in *Maye v. United States*, 2019 U.S. App. LEXIS 12650 (11th Cir. 2019), filed April 25, 2019 affirming the district court's order denying his petition for a writ of *coram nobis*.

OPINION BELOW

The decision and order of the Eleventh Circuit as well as the underlying district court order are included in the Appendix, *infra*.

JURISDICTION

This Court has jurisdiction to review the April 25, 2019 decision of the United States Court of Appeals for the Eleventh Circuit affirming the district court's order denying his petition for a writ of *coram nobis* pursuant to Title 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISIONS INVOLVED

Article One Section Nine of the United States Constitution provides:

> No Bill of Attainder or ex post facto Law shall be passed.

The Fifth Amendment to the United States Constitution provides:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

FEDERAL STATUTE INVOLVED

18 U.S.C. § 1030—Fraud and Related activity in connection with computers

> (a) Whoever—
>
> > (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
> >
> > > (B) information from any department or agency of the United States. . . .

STATEMENT OF THE CASE

Charles Daniel Maye ("Maye" or "Petitioner") was charged, tried and convicted on a superseding indictment filed December 6, 2004 in federal district court for the Middle District of Florida in Case Number 8:04-CR-321-T-30EAJ. Count one charged conspiracy from April 1996 through April 2004:

> to intentionally access a computer without authorization and in excess of authorization and thereby obtain information from any department or agency of the United States, for the purpose of private financial gain and in furtherance of criminal and tortious acts in violation of the Constitution and laws of the United States and the State of Florida, that is, extortion . . .

Count two charged that Maye on July 30, 1999:

> did intentionally access the NCIC computer database without authorization and in excess of authorization, and did thereby obtain information from a department and agency of the United States, for the purpose of private financial gain and in furtherance of criminal and tortious acts in violation of the Constitution and laws of the United States and the State of Florida. All in violation of Title 18, United States Code, Sections 1030(a)(2)(B) and 1030(c)(2)(B)(i) and (ii).

Maye was not charged in count three. Count four charged that Maye on August 11, 2003:

> did intentionally access the NCIC computer database without authorization and in excess of authorization, and did thereby obtain information from a department and agency of the United States, for the purpose of private financial gain and in furtherance of criminal and tortious acts in violation of the Constitution and laws of the United States and the State of Florida. All in violation of Title 18, United States Code, Sections 1030(a)(2)(B) and 1030(c)(2)(B)(i) and (ii).

Count five charged that Maye on April 30, 2004:

> [I]n a matter within the jurisdiction of the Federal Bureau of Investigation, an agency of the executive branch of the Government of the United States, did knowingly and willfully make materially false, fictitious and fraudulent statements and representations, during

> an interview with a Special Agent of the Federal Bureau of Investigation in connection with a criminal investigation, that is, he stated:
>
> [among other matters] [LEROY] COLLINS never asked him to find out any intelligence and that he told COLLINS he wouldn't [and] he accessed information regarding Veronica Smith in the NCIC database in an attempt to locate Veronica Smith's current address and whereabouts for COLLINS, and not to see if Veronica Smith was wanted
>
> [when he] well knew: [LEROY] COLLINS requested MAYE on numerous occasions to obtain information or "intelligence" contained within the NCIC and FCIC databases, and he, in fact, obtained and provided that information to COLLINS;

Maye was a Deputy Sheriff with the Hillsborough County Sheriff's Office at the time of the alleged offenses and used the computer terminal in his patrol car to access the information. There was no dispute that he had the right to access such information as a deputy sheriff. The Government's theory of the case was that he did so in violation of the policy of the sheriff's office with respect to the authorized use of such data and that by violating the policy of the sheriff's office he had violated the "exceeds authorized access" provision of CFAA. Maye was tried by jury, convicted, sentenced to 96 months imprisonment, and served his sentence. Maye has filed various post-conviction challenges to his conviction, all of which have been denied. Maye then filed pursuant to 28 U.S.C. § 1651(a) a

Petition for Writ of Error *Coram Nobis* on June 1, 2017 arguing that his convictions for CFAA violations were based on conduct that is not a crime under the charged statute and did not constitute a legitimate offense against the United States. [Appx. A, excluding exhibits][1] That Petition was summarily denied by the district court on February 16, 2018. [Appx. B] Maye then filed a Motion to Amend Findings and to Alter or Amend the Judgment [Appx. C] and a Request for Remand for Evidentiary Hearing on March 16, 2018. [Appx. D] Both of those motions were denied by the district court on May 23, 2018. [Appx. E] Maye timely filed a Notice of Appeal of both the order denying the Petition for Writ of Error *Coram Nobis* and the order denying his Motion to Amend Findings and to Alter or Amend the Judgment and his Request for Remand for Evidentiary Hearing. [Appx. F] On April 25, 2019 the Eleventh Circuit Court of Appeals issued a *per curiam* order affirming the district court's order denying Maye's petition for a writ of *coram nobis*. [Appx. G]

[1] Bracketed references in the form [Appx.] followed by a letter are to the Appendix accompanying this petition.

ARGUMENT IN SUPPORT OF GRANTING THE WRIT

Whether "exceeds authorized access" in the Computer Fraud Abuse Act ("CFAA") is limited to violations of restrictions on access to information, and not restrictions on its use.

Maye argues that the phrase "exceeds authorized access" in the CFAA does not extend to violations of use restrictions. If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly. The rule of lenity requires "penal laws . . . to be construed strictly." *United States v. Wiltberger*, 18 U.S. (5 Wheat.) 76, 95 (1820). "[W]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *Jones v. United States*, 529 U.S. 848, 858 (2000) (internal quotation marks and citation omitted).

The rule of lenity not only ensures that citizens will have fair notice of the criminal laws, but also that Congress will have fair notice of what conduct its laws criminalize. Criminal statutes must be narrowly construed so that Congress will not unintentionally turn ordinary citizens into criminals. "[B]ecause of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity." *United States v. Bass*, 404 U.S. 336, 348, 92 S. Ct. 515 (1971). "If there is any doubt about whether Congress intended [the CFAA] to

prohibit the conduct in which [Maye] engaged, then 'we must choose the interpretation least likely to impose penalties unintended by Congress.'" *United States v. Cabaccang*, 332 F.3d 622, 635 n.22 (9th Cir. 2003) (quoting *United States v. Arzate-Nunez*, 18 F.3d 730, 736 (9th Cir. 1994)).

This narrower interpretation is also a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere. Therefore, Maye argues that "exceeds authorized access" in the CFAA is limited to violations of restrictions on access to information, and not restrictions on its use.

Maye argues that the conduct alleged by the Government in its indictment did not violate the statute, because Maye was authorized to access the database he accessed and even if it were done with a bad purpose or in contravention of agency policy, that did not constitute an access in excess of the authorized use.

SPLIT IN THE CIRCUITS

Three Circuit Courts of Appeal agree with Maye's interpretation of the statute, the Second, Fourth and Ninth Circuits. Four Circuits disagree, including the Eleventh Circuit.[2]

---

[2] *See United States v. John*, 597 F.3d 263 (5th Cir. 2010); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *Int'l*

Judge Alex Kozkinski, writing for the *en banc* majority of the Ninth Circuit, held:

> We need not decide today whether Congress *could* base criminal liability on violations of a company or website's computer use restrictions. Instead, we hold that the phrase "exceeds authorized access" in the CFAA does not extend to violations of use restrictions.

Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). The United States Army Court of Military Appeals declined to decide the issue but noted the Circuit split:

> The military judge found 18 U.S.C. § 1030(a)(1) to be ambiguous. She applied lenity and rejected the broad approach. The military judge did not consider appellant's purpose or appellant's transmission of the information to Wikileaks as proof of "exceeding authorized access." She found how appellant accessed the information violated the authorized use policy and thus exceeded access. We need not decide which interpretation, narrow or broad, applies to military courts. Here the military judge followed the narrow approach and found appellant's conduct to be an access violation. We agree this was an access violation as discussed below. Appellant's argument conflates "use" violation with "access" violation. Appellant argues that any access restriction must be code-based or technical. We do not read that requirement into the statute. This case does not hinge on a violation in the use of information—nor did the military judge find a use violation. Rather, the method and manner in which appellant accessed the classified State Department system exceeded her authorization.

United States v. Manning, 78 M.J. 501, 512 (A. Ct. Crim. App. 2018).

United States v. Nosal, 676 F.3d 854, 863-64 (9th Cir. 2012) (*en banc*).

The Fourth Circuit, in an opinion authored by Judge Floyd and joined in by Judges Shedd and Hamilton, similarly limited the scope of § 1030's "exceeds authorized access" to apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access:

> Thus, faced with the option of two interpretations, we yield to the rule of lenity and choose the more obliging route. . . . Here, Congress has not clearly criminalized obtaining or altering information "in a manner" that is not authorized. Rather, it has simply criminalized obtaining or altering information that an individual lacked authorization to obtain or alter.
>
> And lest we appear to be needlessly splitting hairs, we maintain that the *Nosal* panel's interpretation would indeed be a harsher approach. For example, such an interpretation would impute liability to an employee who with commendable intentions disregards his employer's policy against downloading information to a personal computer so that he can work at home and make headway in meeting his employer's goals. Such an employee has authorization to obtain and alter the information that he downloaded. Moreover, he has no intent to defraud his employer. But under the *Nosal* panel's approach, because he

> obtained information "in a manner" that was not authorized (i.e., by downloading it to a personal computer), he nevertheless would be liable under the CFAA. *See* § 1030(a)(2)(C). Believing that Congress did not clearly intend to criminalize such behavior, we decline to interpret "so" as "in that manner."
>
> In so doing, we adopt a narrow reading of the terms "without authorization" and "exceeds authorized access" and hold that they apply only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access.

WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 205-07 (4th Cir. 2012).

The Second Circuit joined the Fourth and Ninth Circuits applying a rule of lenity analysis and limiting § 1030's exceeds authorized access in the same manner:

> We agree with the Ninth and Fourth Circuits that courts that have adopted the broader construction "looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of 'exceeds authorized access.'" *Nosal*, 676 F.3d at 863; *see also Miller*, 687 F.3d at 206 ("[W]e believe that th[is] theory has far-reaching effects unintended

> by Congress."). This is the very concern at the heart of the rule of lenity.

United States v. Valle, 807 F.3d 508, 527-28 (2d Cir. 2015).

Although the Eleventh Circuit, in *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), held that exceeds authorized use applied to a government employee's accessing data he was otherwise entitled to access, but did so in violation of agency policy, the Eleventh Circuit Court's opinion contained no analysis of the statute, its legislative history, rule of lenity, or any of the policy concerns addressed by the Second, Fourth and Ninth Circuits. *Rodriguez* is ripe for reconsideration in light of the arguments in support of the holdings in *Nosal*, *WEC* and *Valle*.

STATUTORY TEXT AND STRUCTURE

Maye was charged with misappropriation of the information that was otherwise lawfully available to him as a deputy authorized to use the mobile data terminal in his patrol vehicle. A straightforward reading of the statutory text suggests that Congress did not intend to cover acts of misappropriation. In the text itself, Congress offered the following definition of the phrase "exceeds authorized access": "[T]he 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." 18 U.S.C. § 1030(e)(6). The most natural reading of that language required

dismissal of the relevant counts. Again, the gist of the government's allegation in this case was not that Maye obtained information that he was not entitled to obtain—rather, its allegation was that Maye misused that information.

As many courts have recognized, "the plain language of § 1030(a)(2), (4), and (5)(A)(iii) target the unauthorized procurement or alteration of information, not its misuse or misappropriation." *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (internal quotation marks omitted); *see also Orbit One Communs. v. Numerex Corp*., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ("The plain language of the CFAA supports a narrow reading. The CFAA expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation.").

The government, however, has argued that the statutory term "entitled" implicitly contains a misappropriation theory of liability. According to the government's view of the statute, when an employee obtains information for improper purposes, he loses his "entitlement" to obtain that information. The problem with the government's argument is that it conflates the two prongs of the CFAA. The words "authorize" and "entitle" are synonymous. If improper purpose somehow automatically revoked authorization, then acting "without authorization" and "exceeding authorization" would be coextensive. *See Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342-43 (D. Ga. 2007) (explaining how the "entitlement" theory of misappropriation liability "conflates the meaning of those two

distinct phrases and overlooks their application in § 1030(e)(6)"). The government's reading of the statute would disrupt the two-pronged structure chosen by Congress. In sum, the statutory text and structure of the CFAA support a narrower reading than the one proposed by the government. The text and structure support the result argued by Maye.

LEGISLATIVE HISTORY

The government has also argued that the legislative history of the statute supports a broad reading. Specifically, the government has relied on the Senate Report from the Judiciary Committee explaining the 1986 amendment to the statute. *See* S. Rep. No. 99-432 (1986). A more careful reading of that Report, however, supports the opposite position.

The first version of the CFAA covered not only access without authorization but also access with authorization "for purposes to which such authorization does not extend." In other words, the original statute appeared to cover (among other things) acts of misappropriation. In 1986, Congress replaced that language with the current "exceeds authorized access" language, as well as the definition provided in § 1030(e)(6). Relying on the 1986 Senate Report, the government has argued that the current version is the same as the earlier version and that the amendment had no substantive effect.

A closer examination of the Senate Report, however, suggests that Congress replaced the earlier

language precisely because it was too broad. Senators Mathias and Leahy appended their own statement to the Report and explained in more detail the reason for the 1986 amendments. They explained how the original version of the CFAA had been passed in haste, as part of a legislative rider. *See* S. Rep. No. 99-432, at 21 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2494). As a result, in 1984, the House had never voted on a series of narrowing amendments, which had been unanimously approved by the Senate. The purpose of the 1986 amendments was to fix the shortcomings of the original version. *See id*.

Specifically, Congress replaced the earlier improper "purposes" language precisely to "remove[] from the sweep of the statute one of the murkier grounds of liability." *Id*. In short, as Senators Mathias and Leahy explained, one of the principle purposes of the 1986 amendment was to exclude a misappropriation theory of liability and replace it with something both more narrow and less vague. *See Gast*, 535 F. Supp. 2d at 966 ("The legislative history confirms that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information."); *Int'l Ass'n of Machinists & Aero. Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005) (discussing the 1986 Senate Report and concluding that the amendment was intended to narrow the scope of the statute).

Thus, even if the text itself were not clear, the legislative history demonstrates that the current version of the CFAA was not intended to cover acts of employee misappropriation.

THE CFAA AND THE FAIR WARNING REQUIREMENT

Perhaps most importantly the application of the fair warning requirement would compel a narrow reading of the statute. Criminal laws must be clear so that citizens may know what conduct is forbidden and what conduct is allowed. This principle, which is derived from the Ex Post Facto Clause and the Due Process Clause, is known as the fair warning requirement. As this Court has explained, it has several specific doctrinal components.

> There are three related manifestations of the fair warning requirement. First, the vagueness doctrine bars enforcement of a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application. Second, as a sort of junior version of the vagueness doctrine, the canon of strict construction of criminal statutes, or rule of lenity, ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered. Third, although clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute, due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope. In each of these guises, the touchstone is whether the statute, either standing alone or as construed, made it reasonably clear at the

> relevant time that the defendant's conduct was criminal.

United States v. Lanier, 520 U.S. 259, 266-67 (1997) (citations and internal quotation marks omitted).

VARYING INTERPRETATIONS BY COURTS

The Computer Fraud and Abuse Act is susceptible to a variety of different interpretations. Courts around the country have issued widely varying rulings regarding the statute's scope. If the government's proposed construction were accepted, the statute would cover a remarkably broad range of conduct, including conduct that is not seriously culpable. Such a broad construction would render the statute unconstitutionally vague. Thus, the only way to save the statute is to interpret it narrowly—in precisely the way those courts have done which have limited its application as Maye argues must be done.

DIFFICULTIES IN APPLYING A MISAPPROPRIATION THEORY

The government's legal theory thus appears to be that any employer can create federal criminal liability for misappropriation simply by establishing a corporate or department policy saying that computers may be used for the employer's business only. If that legal theory were accepted, it would raise innumerable problems of application. Professor Kerr explained why:

> Interpreting the CFAA to prohibit employee access of an employer's computer for reasons outside the employment context runs afoul of [the fair warning requirement]. First, the theory gives employees insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited. The key consideration seems to be motive, but the employee has no way to determine what motives are illicit—and in the case of mixed motives, what proportion are illicit. Is use of an employer's computer for personal reasons always prohibited? Sometimes prohibited? If sometimes, when? And if some amount of personal use is permitted, where is the line? If use of an employer's computer directly contrary to the employer's interest is required, how contrary is directly contrary? Is mere waste of the employee's time enough? The cases generally deal with the dramatic facts of an employee who accessed a sensitive and valuable database to gather data that could be used to establish a competing company. But how sensitive does the database need to be? How valuable does the data need to be?

Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1586 (2010).

What is clear is that the government's proposed interpretation of the CFAA would criminalize an astonishingly wide variety of routine employee behavior. It is inconceivable that Congress intended such a result. The fair warning requirement does not allow courts to

reach such a result in the absence of much clearer direction from Congress. Therefore, the Due Process Clause and Ex Post Facto Clause of the Constitution prohibit the application of the statute as was done in Maye's case.

CONCLUSION

WHEREFORE, the Petitioner, Charles Maye, respectfully requests this Honorable Court grant this petition for certiorari.

Respectfully submitted,

KENT & MCFARLAND,
ATTORNEYS AT LAW
WILLIAM MALLORY KENT
24 North Market Street,
Suite 300
Jacksonville, Florida 32202
(904) 398-8000 Telephone
(904) 348-3124 Fax
kent@williamkent.com Email
Counsel for Petitioner Maye