No. 09-4321

IN THE
UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
Appellee

v.

ELAINE ROBERTSON CIONI,
Appellant

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTICT OF VIRGINIA

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS SUPPORTING THE APPELLANT AND URGING REVERSAL

Thomas K. Maher
North Carolina Office of Indigent Services
123 W. Main St.
Suite 400
Durham, NC 27701
(919) 560-3380
(919) 560-3332 – facsimile

Lee Tien
Jennifer Stisa Granick
Marcia Hofmann
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 – facsimile

Attorneys for *Amici Curiae*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Federal Rule of Appellate Procedure 26.1, *amicus* Electronic Frontier Foundation, a 501(c)(3) non-profit corporation incorporated in the Commonwealth of Massachusetts, and *amicus* National Association of Criminal Defense Lawyers, a 501(c)(3) non-profit corporation incorporated in the District of Columbia, make the following disclosures:

1. *Amici* are not publicly held corporations or other publicly held entities.

2. *Amici* have no parent corporations.

3. No publicly held corporation or other publicly held entity owns 10% or more of *amici*.

By: /s/Lee Tien August 5, 2010
Lee Tien
Electronic Frontier Foundation

STATEMENT OF *AMICI CURIAE*

Amici are non-profit public interest organizations seeking to ensure the proper application of the Computer Fraud and Abuse Act and constitutional protections for criminal defendants.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights in the online world. As part of that mission, EFF has served as counsel or amicus in key cases addressing electronic privacy statutes and the Fourth Amendment as applied to the Internet and other new technologies. With more than 14,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to websites in the world, www.eff.org.

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit corporation and the only national bar association working in the interest of public and private criminal defense attorneys and their clients. Founded in 1958, NACDL was established to ensure justice and due process for the accused; to foster the integrity, independence, and expertise of the criminal defense profession; and to promote the proper and fair administration of justice. NACDL has a membership of more than 10,000 direct members worldwide — who are joined by 90 state, local, and international affiliate organizations with more than 35,000 members. NACDL members include private criminal defense lawyers, public defenders, military defense counsel, and law professors who are committed to preserving fairness and due process in criminal justice everywhere.

NACDL has a significant interest in guaranteeing criminal defendants their rights under the Double Jeopardy Clause, which is the central issue addressed in this brief. NACDL urges this Court to fortify that right.

Counsel for Appellant Elaine Cioni and Appellee United States of America have consented to the filing of this brief.

I. INTRODUCTION AND SUMMARY OF ARGUMENT

This case presents a simple question: when a person accesses another's stored email without authorization, may that single act be the basis for both an underlying misdemeanor and a felony enhancement? The answer is no. The Fifth Amendment Double Jeopardy Clause prohibits multiple punishments for the same conduct, and Congress intended the specific conduct at issue here to be punished as a misdemeanor.

The Computer Fraud and Abuse Act ("CFAA") imposes misdemeanor punishments for first-time offenders unless the crime is committed for commercial advantage, financial gain, or for the purpose of committing a criminal or tortious act. But here, the district court convicted a first-time offender of two felonies simply for gaining unauthorized access to certain emails. The government argued and the jury found that the CFAA violations were committed in furtherance of violations of the Stored Communications Act ("SCA"), which also generally provides misdemeanor penalties for unauthorized access to communications in electronic storage. Yet both the underlying CFAA convictions and the felony enhancement were based on identical conduct.

Elaine Cioni's CFAA misdemeanor conduct may not be elevated to a felony merely because the information she was not authorized to access was stored email. The offense was not committed "in furtherance" of a SCA offense, but rather is factually identical to a SCA offense. The government's attempt to count the same conduct as both an underlying misdemeanor and the basis for felony punishment violates the Constitution's Double Jeopardy Clause.

Furthermore, Congress has made clear that harsh penalties are reserved for repeat offenders and those whose conduct is particularly egregious. Cioni's conduct does not rise to this level. Congress made a deliberate choice to punish certain acts as misdemeanors and others as felonies. The prosecution cannot

substitute its own judgment about criminal punishment for that of Congress. Using the same act that underlies the criminal charge to also justify a felony enhancement would eviscerate the misdemeanor penalties in both the CFAA and the SCA.

The CFAA is increasingly recognized as an incredibly broad statute that could be used to improperly criminalize a wide variety of online activities. The government seeks to extend the CFAA's reach even further by making every unauthorized access to stored email a felony. This Court should reject this attempt to broaden the CFAA beyond the statutory penalties Congress has explicitly established, and reduce Cioni's felony CFAA convictions to misdemeanors.

II. STATEMENT OF THE CASE

This case concerns defendant Elaine Cioni's conviction for crimes committed in the course of harassing her former lover and his wife. Cioni was convicted on five felony charges. Only two of these charges — Counts 2 and 4 — are the subject of this brief.

Count 2 of the Superseding Indictment claims that on numerous occasions between November 2006 and March 2008, Cioni gained unauthorized access and exceeded authorized access to AOL's email servers and obtained Maureen Enger's unopened emails. (J.A. 37.) Count 4 alleges that on March 12, 2008, Cioni gained unauthorized access and exceeded authorized access to an AOL computer and obtained messages in Patty Freeman's email account. (J.A. 39.)

Counts 2 and 4 are misdemeanor offenses under either the CFAA or the SCA. However, Cioni was convicted of felony violations of the CFAA, which prohibits unauthorized access or exceeding authorized access to information on a protected computer, in furtherance of violating the SCA, which prohibits unauthorized access or exceeding authorized access to a facility through which an electronic communications service is provided, and thereby obtaining access to

wire or electronic communications in electronic storage. 18 U.S.C. § 2701(a).[1] Because the acts of access, the protected computers, and the information obtained as part of the crime of conviction were identical to the elements of the crime that the offense was allegedly in furtherance of, the felony enhancements violated the Double Jeopardy Clause and were contrary to law. The convictions on these counts should be reversed.[2]

III. ARGUMENT

Cioni should properly have been convicted of two misdemeanor CFAA violations. In the absence of aggravating factors, both the underlying CFAA convictions and any unauthorized access to stored email are punishable as misdemeanors. *See* 18 U.S.C. § 1030(a)(2) (obtaining information from a protected computer via intentional unauthorized access or access exceeding authorization is punishable as a misdemeanor as set forth in § 1030(c)(2)(A)); *see also* 18 U.S.C. § 2701(a) (obtaining, altering or preventing stored electronic communication via

---

[1] "Electronic storage" is a term of art under the SCA, not necessarily encompassing any and all stored messages. *See* 18 U.S.C. § 2510(17). Courts have disagreed about the scope of the definition. *Compare Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004) (messages stored for back-up purposes on ISP server fall under the SCA) *with Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part, vacated in part, and remanded*, 352 F.3d 107 (3d Cir. 2003) (post-transmission storage does not implicate SCA). This disagreement is immaterial for the purposes of *amici*'s argument, however. For the sake of simplicity, we refer more colloquially to communications protected under section 2701 of the SCA as "stored emails" or "stored communications" rather than the more legally accurate "emails/communications in electronic storage."

[2] Cioni was also convicted of a felony on Count 1 for conspiring to violate the CFAA in furtherance of violating the SCA. Because the CFAA offenses should have been misdemeanors, Cioni should have been convicted of a misdemeanor on that count, as well. 18 U.S.C. § 371 ("If . . . the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor.")

intentional unauthorized access or access exceeding authority to a facility through which electronic communications services are provided is punishable as a misdemeanor under section 2701(b)(2)). Despite the legislative determination that a first offender who violates section 1030(a)(2) is generally a misdemeanant, the prosecution obtained felony convictions by alleging that the CFAA violations were committed in furtherance of violations of section 2701. A section 2701 violation, however, will almost always be functionally equivalent to the underlying section 1030 violation where the information obtained is a stored electronic communication, and certainly is true in Cioni's case. Because double counting happened here, Cioni's felony CFAA convictions should be reversed.

A. Cioni's Felony Convictions Under the Computer Fraud and Abuse Act Violate the Fifth Amendment's Double Jeopardy Clause.

A close comparison of the elements of section 1030 and section 2701 shows that the prosecution used the same conduct to prove both the underlying charges and the felony enhancements in this case. This bootstrapping punished Cioni more severely than Congress intended and violated the Fifth Amendment's Double Jeopardy Clause.

1. Identical Facts Underlie the CFAA Convictions and SCA Felony Enhancements.

Cioni was convicted of violating section 1030(a)(2)(C) by accessing or attempting to access Maureen Enger and Patty Freeman's email messages through their AOL accounts. (J.A. 12, 14.) An individual violates section 1030(a)(2)(C) when she "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer[.]" The jury was instructed in and found felony enhancements because the offenses were "committed in furtherance of any criminal act in violation of the

laws of the United States." Jury Instruction No. 19.[3] Furthermore, the jury was told that the enhancing offenses were violations of section 2701(a) of the SCA. *Id*.

An individual violates the SCA when she "intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system[.]" 18 U.S.C. § 2701(a)(1)-(2). This is also a misdemeanor in the absence of aggravating factors. *Id*. § 2701(b).

It is virtually impossible to violate section 2701(a) without also violating section 1030. The elements of the two crimes are nearly identical. The only difference is that section 2701 specifies that the information must be a

---

[3] Jury Instruction No. 19 provided:

> In order to sustain its burden of proof for the crime of unauthorized access to a protected computer as charged in Counts Two and Four of the Superseding Indictment, the government must prove the following essential elements beyond a reasonable doubt:
>
> One: That the defendant intentionally accessed [and attempted to access] a computer without authorization and exceeded [and attempted to exceed] authorized access to a computer;
>
> Two: That the defendant thereby obtained [and attempted to obtain] information from a protected computer;
>
> Three: That the conduct involved an interstate or foreign communication; and
>
> Four: That the offense was committed in furtherance of any criminal act in violation of the laws of the United States.
>
> The criminal act that the defendant is alleged to have furthered by illegally accessing the computer referred to in Counts Two and Four is Title 18, United States Code, Section 2701, which makes it unlawful in some circumstances to accessed stored communications of another person.

communication in electronic storage. Since most access to such communications will also constitute access to a computer, most section 2701 violations are also CFAA violations. This is true here. The underlying offenses and the felony enhancements contain elements that are violated by identical conduct, as the following chart shows.

Comparison of the Elements of 18 U.S.C. § 1030 and 18 U.S.C. § 2701 in This Case

	Elements of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C)	Elements of the Stored Communications Act, 18 U.S.C. § 2701(a)	Facts of This Case Satisfying Elements of Both Statutes
1	"Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access"	"Whoever intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility"	Cioni intentionally accessed or attempted to access the AOL email accounts of Patty Freeman and Maureen Enger without their authorization. The emails were stored on AOL's servers, which are "protected computers" under the CFAA. AOL's email service is an "electronic communication service" under the SCA.
2	"and thereby obtains information"	"and thereby obtains, alters, or prevents authorized access to a wire or electronic communication"	Cioni obtained emails from the email accounts, which are both information and electronic communications.
3	"from any protected computer"	"while it is in electronic storage in such system"	The emails were stored on AOL servers, which are protected computers under the CFAA. The AOL computers also kept the emails in electronic storage within the system.

First, both crimes require intentional access without authorization or in excess of authorization. The Department of Justice recognizes that "intentional access" has a similar mens rea requirement under the CFAA and SCA. U.S. Dep't of Justice, Computer Crime & Intellectual Prop. Section, Prosecuting Computer Crimes 77-78 (2007) (hereinafter "Prosecuting Computer Crimes") (citing courts' interpretation of the mens rea requirement for section 1030 to help explain the similar requirement under section 2701).[4]

Second, in the case of the CFAA, the intentional access must be to a "protected computer." 18 U.S.C. § 1030(a)(2)(C). The definition of "protected computer" is very broad. It is defined as any "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]" 18 U.S.C. § 1030(e)(1) (emphasis added). Any computer that is used to communicate with a website satisfies these requirements. *United States v. Drew*, 259 F.R.D. 449, 457 (C.D. Cal. 2009). In the SCA, intentional access must be to a "facility through which an electronic communication service is provided."[5] 18 U.S.C. § 2701(a)(1); *see* Prosecuting Computer Crimes 11 (a defendant may satisfy section 1030's intentional access element by knowingly "access[ing] a portion of a computer or computer network to which [he has] not been granted

---

[4] *Available at* http://www.justice.gov/criminal/cybercrime/ccmanual/index.html.

[5] Under the Electronic Communications Privacy Act (of which the SCA is a part), an "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications[.]" 18 U.S.C. § 2510(15). An "electronic communication," in turn, is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," with certain exceptions not applicable here. *Id*. § 2510(12).

access"); *Id*. at 78 (a defendant may satisfy section 2701's element of accessing a facility that provides an electronic communications service by "logging on to an email server"). Here, AOL's email servers satisfy both definitions because they are computers, and they are also part of a network through which an electronic communication service is provided.

Finally, both crimes require obtaining information. The relevant provision of the CFAA prohibits one from intentionally accessing a protected computer without authorization or in excess of authorization and thereby obtaining "information from any protected computer if the conduct involved an interstate or foreign communication[.]" 18 U.S.C. § 1030(a)(2)(C). As the statutory history of the CFAA makes clear, the phrase "obtaining information" is a broad term that includes merely reading or observing data. S. Rep. No. 99-432, at 6-7 (1986); S. Rep. No. 104-357, at 7 (1996). The SCA requires "obtain[ing] . . . [un]authorized access to a wire or electronic communication . . . in electronic storage," 18 U.S.C. § 2701(a)(2), a requirement that is also met by "obtaining information" within the meaning of the CFAA. In short, accessing unopened emails in another person's email account satisfies both definitions of information protected under each statute.

For these reasons, SCA violations will almost always also be CFAA violations. Indeed, the Department of Justice acknowledges that an individual who wrongfully obtains access to a communication in electronic storage has often also completed a violation of the CFAA. Prosecuting Computer Crimes 84 ("[M]any violations of section 2701 also involve conduct that violates 18 U.S.C. § 1030.").[6]

---

[6] Importantly, the Superseding Indictment originally included a count alleging that Cioni violated the SCA, 18 U.S.C. §§ 2701(a)(1), (a)(2) & (b)(1)(A), by "gain[ing] and attempt[ing] to gain unauthorized access to the AOL account of [Patty Freeman], located on a computer operated by AOL within the Eastern District of Virginia, and obtained and attempted to obtain unopened electronic mail messages in [Freeman's] account by means of electronic communications." (J.A.

Here, the CFAA violations and the SCA felony enhancements are one and the same. Cioni accessed AOL's servers when she attempted to access or accessed Maureen Enger and Patty Freeman's email messages through their AOL accounts. The conduct that allegedly violated section 1030 is the same conduct that would violate section 2701.

2. Cioni's Felony Convictions Violate the Double Jeopardy Clause.

The prosecution here improperly inflated two section 1030 violations for unauthorized access to information into felonies despite legislative enactments to the contrary. The government did not prove that Cioni's section 1030 offenses were committed in furtherance of separate crimes. Rather, it effectively argued that because her misdemeanor conduct could also have been prosecuted under a different misdemeanor statute, she committed a felony. But two misdemeanor offenses do not make a felony. Cioni's conviction imposes greater punishment than authorized by Congress. As such, it violates the Double Jeopardy Clause.

The Double Jeopardy Clause reads, "[no person shall] be subject for the same offense to be twice put in jeopardy of life or limb." U.S. Const. Amend. V, cl. 2. It "protects against a second prosecution for the same offense after acquittal. It protects against a second prosecution for the same offense after conviction. And it protects against multiple punishments for the same offense." *North Carolina v. Pearce*, 395 U.S. 711, 717 (1969) (footnotes omitted). When the legislature has declared that a given offense is a misdemeanor, the prosecution cannot evade that legislative determination by improperly using the elements of the misdemeanor both to prove the crime and also to elevate the crime to a felony.

The double jeopardy analysis is relatively simple: were the underlying section 1030 violation and the alleged section 2701 violation one offense for

---

at 38.) The government moved to dismiss this charge prior to voir dire, which the district court granted. (J.A. at 13.)

constitutional purposes, and if so did Congress clearly intend that the one misdemeanor offense be punishable as a felony? Only if the alleged violations are constitutionally separate crimes, or if Congress clearly intended the enhanced punishment for the single offense, could the felony convictions pass muster under the Double Jeopardy Clause.

The fact that a violation of section 2701 is covered by a separate statute is irrelevant to determining whether that violation is a separate offense from a violation of section 1030. In *Blockburger v. United States*, the Court held:

> The applicable rule is that where the same act or transaction constitutes a violation of two distinct statutory provisions, the test to be applied to determine whether there are two offenses or only one, is whether each provision requires proof of a fact which the other does not.

284 U.S. 299, 304 (1932). The fact that a defendant's acts violate two separate statutes does not preclude a finding that the act is but one offense. If the violation of one of the statutes cannot be accomplished without violating the other, then the act is only one crime.

The double jeopardy test is the same regardless of whether the government seeks to prosecute in successive trials, or seeks increased punishment for multiple convictions in a single trial:

> If two offenses are the same under this test for purposes of barring consecutive sentences at a single trial, they necessarily will be the same for purposes of barring successive prosecutions. *See In re Nielsen*, 131 U.S. 176, 187-188 (1889); cf. *Gavieres v. United States*, 220 U.S. 338 (1911). Where the judge is forbidden to impose cumulative punishment for two crimes at the end of a single proceeding, the prosecutor is forbidden to strive for the same result in successive proceedings. Unless "each statute requires proof of an additional fact which the other does not," *Morey v. Commonwealth*, 108 Mass. 433, 434 (1871), the Double Jeopardy Clause prohibits successive prosecutions as well as cumulative punishment.

Brown v. Ohio, 432 U.S. 161, 166 (1977).

In this case, the government could not have prosecuted Cioni for attempting

to access Freeman's email under section 1030 in one trial, and then bring a second indictment using the same facts to allege a violation of section 2701. It follows that the government cannot bootstrap the two offenses to inflict a harsher punishment upon Cioni than either statute alone would permit.

A closer look at Count 4 illustrates the prosecution's double counting. Count 4 was based upon a single attempted access to Freeman's AOL email. The government specifically argued that the felony enhancement was established if Cioni accessed AOL's servers in order to obtain an unread email:

> Well, the government has also proved beyond any reasonable doubt a fourth element, and that is indicated on our chart by access to e-mail, that the defendant's access into these protected computers in this district were done for a purpose, in furtherance of. And what is that in furtherance of? To getting an unread e-mail.

Trial Tr. 161:16-22, Dec. 11, 2008. The access to AOL servers and the attempt to access Freeman's email are inarguably one and the same act.

The jury instructions exacerbated rather than resolved the matter. They merely informed the jury that the fourth element of each section 1030 offense — the element that elevated the crime to a felony — was that that the offense be in furtherance of a violation of section 2701. Jury Instruction No. 19. The instruction did not require the jury to find violations of section 2701 separate from the violations of section 1030, and nothing in the instruction on the elements of section 2701 identified any act separate or distinct from the underlying section 1030 violations. Furthermore, the jury was not instructed that it could only convict of a felony if it found an element that was not already present in the misdemeanor.

One of the core functions of the Double Jeopardy Clause is to ensure that the legislature's decision about the appropriate punishment for a crime is respected by the other branches of government. When the legislature declares that a given offense is a misdemeanor, the prosecution cannot alter that decision by seeking

multiple punishments for one crime, nor may it elevate the offense to a felony by improperly using the elements of the misdemeanor to both prove the crime and elevate the crime to a felony. For these reasons, Counts 2 and 4 should be reversed.

C. The Plain Text and Legislative History of the Computer Fraud and Abuse Act Makes Clear That Congress Did Not Authorize the Government's Double Counting.

The only exception to the ban on seeking enhanced punishment for an act that constitutes a single offense is when the legislature has clearly authorized the enhanced punishment. *Whalen v. United States*, 445 U.S. 684, 692 (1980) ("[W]here two statutory provisions proscribe the 'same offense,' they are construed not to authorize cumulative punishments in the absence of a clear indication of contrary legislative intent."). The Supreme Court examined this exception in *Missouri v. Hunter*, 459 U.S. 359 (1983), in which the defendant was convicted and given consecutive sentences for armed robbery and armed criminal action. Under the applicable state statute anyone who committed a felony with the use of a deadly weapon was guilty of armed criminal action and subject to a sentence to run consecutively with the sentence imposed on the underlying felony. The Missouri courts determined that armed criminal action was constitutionally the same offense as armed robbery as one could not commit armed robbery without also committing an armed criminal action, and that despite the clear legislative intent to require cumulative punishment, such punishment was unconstitutional.

The Supreme Court nonetheless held that cumulative punishment for these convictions was not barred by the Double Jeopardy Clause. Rather, the Court held that "with respect to cumulative sentences imposed in a single trial, the Double Jeopardy Clause does no more than prevent the sentencing court from prescribing greater punishment than the legislature intended." *Id*. at 366. When the legislature has made clear its intent that cumulative punishment be imposed, even when the relevant statutes define only one crime, then double jeopardy imposes no barrier to

that punishment. "Here, the Missouri Legislature has made its intent crystal clear. Legislatures, not courts, prescribe the scope of punishments." *Hunter*, 459 U.S. at 368.

Hunter emphasized the need for clear legislative intent before a court would approve enhanced punishment based upon multiple convictions for the same offense. *See also Albernaz v. United States*, 450 U.S. 333, 340 (1981) ("[the] *Blockburger* test is a 'rule of statutory construction,' and because it serves as a means of discerning congressional purpose the rule should not be controlling where, for example, there is a clear indication of contrary legislative intent.").

In both the CFAA and SCA, Congress set forth a thoughtful regime of lesser penalties for first-time and minor offenses, and harsher penalties for more severe violations of the statutes. 18 U.S.C. § 1030(c); 18 U.S.C. § 2701(b). The structure of these statutes makes clear that Congress envisioned that a first offender who does no more than improperly access emails on a protected computer is guilty of a misdemeanor under this statutory scheme — not a felony by using one statute to compound the effect of the other.[7]

When Congress enacted the 1996 amendments to 18 U.S.C. § 1030(a), Public L. No. 104-294, 110 Stat. 3488, it explicitly indicated its intent that the phrase "for the purpose of committing any criminal or tortious act" should be narrowly construed. S. Rep. No. 104-357, which accompanied S. 982, explained that amendments to section 1030(a)(2)(C) were "intended to protect against the interstate or foreign theft of information by computer," extending the coverage of

[7] Both the CFAA and SCA contain provisions that increase punishment if the statutes are violated under particular circumstances. 18 U.S.C. § 1030(c); 18 U.S.C. § 2701(b). While these alternative provisions are not directly relevant in this case, they reflect the care with which Congress considered punishment in connection with the varying degrees of culpability that can accompany a violation of the statutes.

section 1030(a)(2) to information on federal government computers, and to computers used in interstate or foreign commerce or communications if the conduct involved an interstate or foreign communication.[8] The Senate Report also clarified how the drafters intended such offenses to be punished. Specifically, the report explained:

> The sentencing scheme for section 1030(a)(2) is part of a broader effort to ensure that sentences for section 1030 violations adequately reflect the nature of the offense. Thus, under the bill, the harshest penalties are reserved for those who obtain classified information that could be used to injure the United States or assist a foreign state. Those who improperly use computers to obtain other types of information — such as financial records, nonclassified Government information, and information of nominal value from private individuals or companies — face only misdemeanor penalties, unless the information is used for commercial advantage, private financial gain or to commit any criminal or tortious act.
>
> For example, individuals who intentionally break into, or abuse their authority to use, a computer and thereby obtain information of minimal value of $5,000 or less, would be subject to a misdemeanor penalty. The crime becomes a felony if the offense was committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000.
>
> The terms "for purposes of commercial advantage or private financial gain" and "for the purpose of committing any criminal or tortious act" are taken from the copyright statute (17 U.S.C. 506(a)) and the wiretap statute (18 U.S.C. 2511(1)(d)), respectively, and are *intended to have the same meaning* as in those statutes.

S. Rep. No. 104-357, at 8 (1996) (emphasis added).

While no courts have considered the meaning of the phrase "for the purpose of committing any criminal or tortious act" under the CFAA, many courts have interpreted the same language in the context of the Wiretap Act, 18 U.S.C. § 2511,

[8] H.R. 3723 was ultimately passed in lieu of S. 982, though S. 982 contained proposed amendments to the CFAA that were substantially similar to the language that ultimately became law.

which provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception *unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act.*

18 U.S.C. § 2511(2)(d) (2008) (emphasis added). The courts have uniformly determined that the "criminal or tortious act" cannot be the interception itself. *See, e.g., United States v. Truglio*, 731 F.2d 1123, 1131 (4th Cir. 1984); *By-Prod Corp. v. Armen-Berry Co.*, 668 F.2d 956, 960 (7th Cir. 1982) ("it is the use of the interception with intent to harm rather than the fact of interception that is critical to liability"); *Boddie v. American Broadcasting Companies, Inc.*, 731 F.2d 333, 339 (6th Cir. 1984) ("The Wiretap Statute requires the plaintiff to show that the defendants intended an illegal, tortious or injurious act other than the recording of the conversation."). Indeed, when interpreting similar language in the SCA, the Department of Justice has noted that "[n]aturally, the 'in furtherance of any criminal or tortious act' language means an act *other than the unlawful access to stored communications itself*." Prosecuting Computer Crimes 82 (citing *Boddie*, 731 F.2d 333) (emphasis added).

The judicial interpretations of the phrase "for the purpose of committing any criminal or tortious act" in the Wiretap Act make clear that the criminal or tortious act cannot be the interception itself. The CFAA's legislative history indicates that this language in the CFAA is based on the Wiretap Act. It follows that the phrase "for the purpose of committing any criminal or tortious act" in the CFAA cannot refer to the unauthorized access itself, just as in the Wiretap Act this language cannot refer to the interception itself.

D. If Accepted by the Court, the Government's Position Would Punish Defendants More Severely Than Congress Intended and Give Prosecutors Great Discretion Under an Already Overbroad Statute.

Congress has made clear its intention that a violation of section 1030 should be punished as a misdemeanor where the crime charged is merely accessing personal email accounts and obtaining personal email, as Cioni did here. To elevate this kind of CFAA violation to a felony imposes a far more significant punishment than Congress intended. The difference is important because a felony conviction can have profound consequences for the rest of an individual's life. After serving prison time, felons may have difficulty finding work. They may be prohibited from participating meaningfully in civic life, losing the right to vote in elections, hold public office or be a member of a jury. Non-U.S. citizens who are convicted of felonies may be deported. Particularly because a felony conviction is a life-long burden, the Court should not allow prosecutors the discretion to charge an individual with a felony rather than a misdemeanor where Congress has determined that misdemeanor punishment is appropriate.

Moreover, the government's attempted expansion of the punishments under the CFAA is problematic because courts and academics have noted that the statute is exceptionally broad and, without careful judicial oversight, could be used to criminalize a wide array of routine online activities. *E.g.*, *Drew*, 259 F.R.D. at 466 (rejecting the government's contention that breach of a website's terms of service violates the CFAA, noting that a contrary finding would "transform[] section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals"); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1561 (2010) ("Statutory amendments and the increasing computerization of American society have combined to render the CFAA one of

the most far-reaching criminal laws in the United States Code.").

Under the government's theory in this case, a significant number of internet users who commit relatively minor computer crime offenses could be charged with felonies at the government's whim. For example, a woman who attempts (even unsuccessfully) to check her husband's email without his explicit consent could be charged with a felony at the prosecutor's discretion. A concerned mother who logs into her college-aged son's email account because she has not heard from him in several days might also be accused of a felony. Or if an individual on a library's public computer reads email in an account from which a stranger neglected to log out, he could face substantial prison time. This Court should not give prosecutors such leeway, and instead should narrowly construe statutes that impose criminal penalties in favor of lenity. *See Skilling v. United States*, 177 L. Ed. 619, 661 (2010); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009).

IV. CONCLUSION

Congress made a deliberate choice to create a category of offenses punishable as misdemeanors under both the CFAA and the SCA. Congress's intent has been undermined here. In prosecuting Cioni, the government built felony offenses out of two factually identical misdemeanors. For this reason, the felony convictions in Counts 1, 2 and 4 must be reversed. Any other result violates Cioni's Fifth Amendment rights, and risks aggravating every misdemeanor section 2701 case — and every section 1030 case involving stored email — into a felony. Such an outcome will almost certainly result in increased exercise of prosecutorial discretion under an already worrisomely broad statute.

Date: August 5, 2010

By: /s/Lee Tien

LEE TIEN
JENNIFER STISA GRANICK
MARCIA HOFMANN
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

THOMAS K. MAHER
North Carolina Office of
Indigent Services
123 W. Main St.
Suite 400
Durham, NC 27701

Attorneys for *Amici Curiae*

CERTIFICATE OF COMPLIANCE

This brief has been prepared in 14-point Times New Roman font. This brief contains 5,657 words and complies with the 7,000 word limitation pursuant to Rule 32.

By: /s/Lee Tien
LEE TIEN

CERTIFICATE OF SERVICE

I hereby certify that on August 5, 2010, an electronic copy of the foregoing was served via CM/ECF on:

JENNIFER WICKS The Law Offices Of Jennifer Wicks The Webster Building 503 D Street NW Suite 250A Washington, D.C. 20001	JAY PRABHU U.S. Attorney's Office Eastern District of Virginia 2100 Jamieson Avenue Alexandria, VA 22314
Appointed by the Court for Appellant	Attorney for Appellee

By: /s/Lee Tien
LEE TIEN