

**IN THE UNITED STATES ARMY
COURT OF CRIMINAL APPEALS**

----- x
UNITED STATES, :
 Appellee, :
 : :
 v. : Docket No. ARMY 20130739
 : :
Private First Class (E-3) : Tried at Forth Meade, Maryland,
CHELSEA MANNING, : on 23 February, 15-16 March,
United States Army, : 24-26 April, 6-8, 25 June,
 Appellant. : 16-19 July, 28-30 August, 2,
 : 12, and 17-18 October, 7-8, and
 : 27 November-2, 5-7, and 10-11
 : December 2012, 8-9 and 16
 : January, 26 February-1,
 : 8 March, 10 April, 7-8 and 21
 : May, 3-5, 10-12, 17-18 and 25-
 : 28 June, 1-2, 8-10, 15, 18-19,
 : 25-26, and 28 July-2, 5-9, 12-
 : 14, 16, and 19-21 August 2013,
 : Before a general court-martial
 : Appointed by Commander, United
 : States Army Military District
 : Of Washington, Colonel Denise
 : Lind, Military Judge,
 : presiding.
----- x

**UNOPPOSED MOTION FOR LEAVE TO FILE BRIEF OF AMICI CURIAE
ELECTRONIC FRONTIER FOUNDATION, NATIONAL ASSOCIATION OF CRIMINAL
DEFENSE LAWYERS, AND CENTER FOR DEMOCRACY & TECHNOLOGY IN
SUPPORT OF APPELLANT**

Pursuant to Rule 15.4 of the Court's Internal Rules of Practice and Procedure, the Electronic Frontier Foundation ("EFF"), the National Association of Criminal Defense Lawyers ("NACDL"), and the Center for Democracy & Technology ("CDT") hereby move for leave to file the attached brief of *amici curiae* in support of Appellant Chelsea Manning in the above-captioned matter. Undersigned counsel contacted counsel for both parties seeking their consent to this motion. Appellant's counsel, Nancy

Hollander, consented to the filing of the attached brief, and Appellee's counsel, CPT Christopher A. Clausen, indicated that the government has no objection.

Amici file the attached brief to draw the Court's attention to the significant issues presented by the lower court's application of the federal anti-hacking statute, the Computer Fraud and Abuse Act ("CFAA"). Amici's brief provides the Court with a unique perspective and will assist the Court in understanding the implications of the lower court's decision. Good cause thus exists for this Court to grant Amici's motion for leave.

1. Statement of Interest

EFF is a non-profit, member-supported civil liberties organization working to protect consumer interests, innovation, and free expression in the digital world. With over 24,000 active donors and dues-paying members, EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age, and it publishes a comprehensive archive of digital civil liberties information at www.eff.org. EFF is particularly interested in the principled and fair application of computer crime laws generally and the CFAA specifically. In that regard, EFF has served as counsel or amicus in key cases addressing the CFAA. See *United States v. Valle*, 807 F.3d 508 (2nd Cir. 2015)

(amicus); *United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014) (appellate co-counsel); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) (amicus); *United States v. Cioni*, 649 F.3d 276 (4th Cir. 2011) (amicus); *Craigslist, Inc. v. 3Taps, Inc.*, 964 F. Supp. 2d 1178 (N.D. Cal. 2013) (amicus); *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (amicus).

NACDL is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of approximately 9,000 direct members in 28 countries, and 90 state, provincial and local affiliate organizations totaling up to 40,000 attorneys. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL files numerous amicus briefs each year in the U.S. Supreme Court and other courts, including the military courts, to provide assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole. In furtherance of NACDL's mission to safeguard fundamental constitutional rights, the Association often appears as amicus in cases involving overcriminalization. NACDL is particularly interested in this case given its concerns about the

implications of the overbroad application of criminal laws, including the CFAA.

CDT is a nonprofit public interest group that seeks to promote free expression, privacy, individual liberty, and technological innovation on the open, decentralized Internet. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of Internet users. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

2. Amici Are Not Affiliated With Any Party.

No party's counsel authored this brief in whole or in part, and neither any party, nor any party's counsel, contributed money towards the preparation of this brief. No person other than Amici, its members, or its counsel contributed money that was intended to fund preparing or submitting this brief. EFF has counseled Appellant regarding the receipt of reading materials (unrelated to this case) in prison, but has not counseled Appellant in the above-captioned case or in any other capacity.

3. Amici's Brief Offers a Unique Perspective and Does Not Merely Duplicate the Brief of Appellant.

Finally, Amici's brief does not merely duplicate Appellant's brief. Rather, it provides the Court with a unique and important perspective on the broader policy considerations of the lower

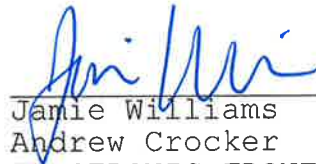
court's application of the CFAA—a perspective not offered by either party. Amici's brief will thus assist the Court in understanding a significant issue presented in this appeal.

4. Conclusion

For the reasons discussed above, Amici respectfully request that this Court grant leave to file the accompanying brief.

Date: San Francisco, California
17 May 2016

Respectfully submitted,



Jamie Williams
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993
jamie@eff.org

*Counsel for Amici Curiae¹
Electronic Frontier Foundation,
National Association of Criminal
Defense Lawyers, and Center for
Democracy & Technology*

¹ Above-listed counsel are not admitted to practice before this Court and therefore request permission, pursuant to Rule 8(c) of the Court of Criminal Appeals Rules of Practice and Procedure, to appear *pro hac vice* for the limited purpose of submitting the attached amicus brief. Good cause exists to grant this request given the serious nature of the issues at stake in this case. Counsel are members in good standing of the bar in California and are admitted to practice before various federal courts.

**IN THE UNITED STATES ARMY
COURT OF CRIMINAL APPEALS**

----- x
UNITED STATES, :
 Appellee, :
 : :
 v. : Docket No. ARMY 20130739
 : :
Private First Class (E-3) : Tried at Fort Meade, Maryland,
CHELSEA MANNING, : on 23 February, 15-16 March,
United States Army, : 24-26 April, 6-8, 25 June,
 Appellant. : 16-19 July, 28-30 August, 2,
 : 12, and 17-18 October, 7-8, and
 : 27 November-2, 5-7, and 10-11
 : December 2012, 8-9 and 16
 : January, 26 February-1,
 : 8 March, 10 April, 7-8 and 21
 : May, 3-5, 10-12, 17-18 and 25-
 : 28 June, 1-2, 8-10, 15, 18-19,
 : 25-26, and 28 July-2, 5-9, 12-
 : 14, 16, and 19-21 August 2013,
 : Before a general court-martial
 : Appointed by Commander, United
 : States Army Military District
 : Of Washington, Colonel Denise
 : Lind, Military Judge,
 : presiding.
----- x

**BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, NATIONAL
ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AND CENTER FOR
DEMOCRACY & TECHNOLOGY IN SUPPORT OF APPELLANT**

Jamie Williams
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415)436-9333
Fax: (415) 436-9993
jamie@eff.org

*Counsel for Amici Curiae
Electronic Frontier Foundation,
National Association of Criminal
Defense Lawyers, and Center for
Democracy & Technology*

Index of Brief

Argument 3

1. The Computer Fraud and Abuse Act Does Not Prohibit
Violations of Computer Use Restrictions, Such as the
Restriction at Issue..... 3

 a) The CFAA was meant to target "hacking," not
 violations of computer use restrictions. 5

 b) Written, policy-based restrictions on manner of
 access are restrictions on use. 12

2. The Lower Court's Broad Reading of the CFAA Renders
the Statute Unconstitutionally Vague..... 19

 a) Corporate policies do not provide sufficient
 notice of what conduct is prohibited. 20

 b) Basing CFAA liability on violations of use
 restrictions would permit capricious enforcement
 by prosecutors. 23

Conclusion 25

Table of Authorities

Cases

Advanced Fluid Systems, Inc. v. Huber,
28 F. Supp. 3d 306 (M.D. Pa. 2014) 10

Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc.,
690 F. Supp. 2d 1267 (M.D. Ala. 2010) 10

Black & Decker, Inc. v. Smith,
568 F. Supp. 2d 929 (W.D. Tenn. 2008) 10

Bouie v. City of Columbia,
378 U.S. 347 (1964) 18

Clarity Servs., Inc. v. Barney,
698 F. Supp. 2d 1309 (M.D. Fla. 2010) 10

Cloudpath Networks, Inc. v. SecureW2 B.V.,
___ F. Supp. 3d ___, 2016 WL 153127 (D. Colo. Jan. 13, 2016) .. 10

Connally v. Gen. Const. Co.,
269 U.S. 385 (1926) 20

Craigslist, Inc. v. 3Taps Inc.,
942 F. Supp. 2d 962 (N.D. Cal. 2013) 15, 16

Craigslist, Inc. v. 3Taps, Inc.,
964 F. Supp. 2d 1178 (N.D. Cal. 2013) 6, 16

Cranel Inc. v. Pro Image Consultants Group, LLC,
57 F. Supp. 3d 838 (S.D. Ohio 2014) 10

Cvent, Inc. v. Eventbrite, Inc.,
739 F. Supp. 2d 927 (E.D. Va. 2010) 7, 14

Diamond Power Int’l., Inc. v. Davidson,
540 F. Supp. 2d 1322 (N.D. Ga. 2007) 10

Dresser-Rand Co. v. Jones,
957 F. Supp. 2d 610 (E.D. Pa. 2013) 10, 11

EF Cultural Travel BV v. Explorica, Inc.,
274 F.3d 577 (1st Cir. 2001) 11

Enhanced Recovery Co., LLC v. Frady,
2015 WL 1470852 (M.D. Fla. Mar. 31, 2015) 10

Experian Marketing Solutions, Inc. v. Lehman,
2015 WL 5714541 (W.D. Mich. Sept. 29, 2015) 10

<i>Giles Const., LLC v. Tooele Inventory Solution, Inc.</i> , 2015 WL 3755863 (D. Utah Jun. 16, 2015)	10
<i>Grayned v. Rockford</i> , 408 U.S. 104 (1972)	23
<i>IBP, Inc. v. Alvarez</i> , 546 U.S. 21 (2005)	17
<i>Int'l Airport Ctrs. v. Citrin</i> , 440 F.3d 418 (7th Cir. 2006)	11
<i>Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda</i> , 390 F. Supp. 2d 479 (D. Md. 2005)	6, 10
<i>Koch Industries</i> , 2011 WL 1775765 (D. Utah May 9, 2011)	14
<i>Kolender v. Lawson</i> , 461 U.S. 352 (1983)	19
<i>Kozminski</i>	24
<i>Lane v. Brocq</i> , 2016 WL 1271051 (N.D. Ill., March 28, 2016)	10
<i>Leocal v. Ashcroft</i> , 543 U.S. 1 (2004)	7, 8
<i>Lewis-Burke Associates, LLC v. Widder</i> , 725 F. Supp. 2d 187 (D.D.C. 2010)	10
<i>LVRC Holdings LLC v. Brekka</i> , 581 F.3d 1127 (9th Cir. 2009)	<i>passim</i>
<i>Milner v. Dep't of Navy</i> , 562 U.S. 562 (2011)	13, 14
<i>Nat'l City Bank, N.A. v. Republic Mortgage Home Loans</i> , 2010 WL 959925 (W.D. Wash. Mar. 12, 2010)	10
<i>Power Equipment Maintenance, Inc. v. AIRCO Power Services, Inc.</i> , 953 F. Supp. 2d 1290 (S.D. Ga. 2013)	10
<i>Pulte Homes, Inc. v. Laborer's Int'l Union of N. Am.</i> , 648 F.3d 295 (6th Cir. 2011)	6
<i>ReMedPar, Inc. v. AllParts Med., LLC</i> , 683 F. Supp. 2d 605 (M.D. Tenn. 2010)	10
<i>Shamrock Foods Co. v. Gast</i> , 535 F. Supp. 2d 962 (D. Ariz. 2008)	10

<i>Skilling v. United States</i> , 561 U.S. 358 (2010)	19
<i>United States v. John</i> , 597 F.3d 263 (5th Cir. 2010)	11
<i>United States v. Kozminski</i> , 487 U.S. 931 (1988)	23, 24
<i>United States v. Lanier</i> , 520 U.S. 259 (1997)	19, 20
<i>United States v. Nosal</i> , 676 F.3d 854 (9th Cir. 2012)	<i>passim</i>
<i>United States v. Rodriguez</i> , 628 F.3d 1258 (11th Cir. 2010)	11
<i>United States v. Santos</i> , 553 U.S. 507 (2008)	11, 19
<i>United States v. Stevens</i> , 559 U.S. 460 (2010)	24, 25
<i>United States v. Valle</i> , 807 F.3d 508 (2nd Cir. 2015)	<i>passim</i>
<i>WEC Carolina Energy v. Miller</i> , 687 F.3d 199 (4th Cir. 2012)	<i>passim</i>
Wentworth-Douglass Hospital v. Young & Novis Professional Association, 2012 WL 2522963 (D.N.H. June 29, 2012)	16, 17

Statutes

18 U.S. Code § 1030, The Computer Fraud and Abuse Act	<i>passim</i>
--	---------------

Other Authorities

Dartmouth College, Employment Policies and Procedures Manual .	22
Employee Handbook	22
Orin S. Kerr, <i>Vagueness Challenges to the Computer Fraud and Abuse Act</i> , 94 Minn. L. Rev. 1561 (2010)	21
Susan M. Heathfield, Internet and Email Policy	22
The American Heritage Dictionary (5th ed.)	4
Virginia Dep't of Human Resource Management, Use of the Internet and Electronic Communications Systems	22

Administrative Cases

1986 U.S.C.C.A.N. 2479 (September 3, 1986) 6

H.R. Rep. 98-894, at 9, 1984 U.S.C.C.A.N. 3689
(July 24, 1984) 5

S. Rep. No. 104-357, at 6 (1996) 13

**IN THE UNITED STATES ARMY
COURT OF CRIMINAL APPEALS**

----- x
UNITED STATES, :
 Appellee, :
 : :
 v. : Docket No. ARMY 20130739
 : :
Private First Class (E-3) : Tried at Fort Meade, Maryland,
CHELSEA MANNING, : on 23 February, 15-16 March,
United States Army, : 24-26 April, 6-8, 25 June,
 Appellant. : 16-19 July, 28-30 August, 2,
 : 12, and 17-18 October, 7-8, and
 : 27 November-2, 5-7, and 10-11
 : December 2012, 8-9 and 16
 : January, 26 February-1,
 : 8 March, 10 April, 7-8 and 21
 : May, 3-5, 10-12, 17-18 and 25-
 : 28 June, 1-2, 8-10, 15, 18-19,
 : 25-26, and 28 July-2, 5-9, 12-
 : 14, 16, and 19-21 August 2013,
 : Before a general court-martial
 : Appointed by Commander, United
 : States Army Military District
 : Of Washington, Colonel Denise
 : Lind, Military Judge,
 : presiding.
-----x

**BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, NATIONAL
ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AND CENTER FOR
DEMOCRACY & TECHNOLOGY IN SUPPORT OF APPELLANT**

The Computer Fraud and Abuse Act ("CFAA"), the federal anti-"hacking" statute, was intended to criminalize the circumvention of technical restrictions in order to access data by a person not otherwise entitled to access it. The statute was not intended to criminalize breaches of contract or the misappropriation or misuse of data. The lower court recognized this, adopting the view of the three most recent federal circuit courts to interpret the CFAA's "exceeds authorized access"

language—that the CFAA must be interpreted narrowly to apply only to violations of access restrictions, i.e., limits on who is “authorized” to access certain information, and not to violations of use restrictions, i.e., limits on how such authorized individuals can use their authorization. See 8 June 2012 Order, 8-9; see also *United States v. Nosal*, 676 F.3d 854, 858-59 (9th Cir. 2012); *WEC Carolina Energy v. Miller*, 687 F.3d 199, 119 (4th Cir. 2012); *United States v. Valle*, 807 F.3d 508, 527-28 (2nd Cir. 2015).

But in holding Appellant criminally liable under Specification 13 of Charge II, the lower court misclassified the type of restriction at issue in this case. Namely, the lower court incorrectly held that Appellant’s use of unauthorized software to access the Department of State’s Net-Centric Diplomacy (“NCD”) database constituted a violation of an “access” restriction. The applicable acceptable use policy (“AUP”) restriction—a written, non-technical, policy-based limit on the “manner” in which Appellant could use her authorization to access information within the NCD database—is in fact merely a type of *use* restriction.

In ruling that Appellant “exceeded authorized access” to the NCD database when she accessed classified information via the use of unauthorized software, the lower court thus found Appellant criminally liable for violating a computer use

restriction. Such an outcome is inconsistent with not only the holdings of the three most recent circuit courts to address the issue, but also the court's own legal conclusions below. And it takes the CFAA far beyond the statute's narrow, intended purpose—punishing “hacking.”

This Court should reverse Appellant's conviction under Specification 13 of Charge II.

Argument

1. The Computer Fraud and Abuse Act Does Not Prohibit Violations of Computer Use Restrictions, Such as the Restriction at Issue.

Section 1030(a)(1) of the CFAA prohibits “knowingly access[ing] a computer *without authorization or exceeding authorized access*, and by means of such conduct . . . obtain[ing] information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations” and “willfully communicat[ing], deliver[ing], transmit[ting]. . . [the information] to any person not entitled to receive it[.]” 18 U.S.C. § 1030(a)(1) (emphasis added). The statute defines the term “exceeds authorized access” as “to access a computer with authorization and to use such access to obtain or alter

information in the computer that the accessor is not entitled so to obtain or alter.”¹ 18 U.S.C. § 1030(e)(6).

The CFAA’s prohibition against accessing a protected computer “without authorization” covers outsiders who have no rights to the computer system, while the prohibition against “exceed[ing] authorized access” is aimed at insiders who “ha[ve] permission to access the computer, but access[] information on the computer that the[y] [are] not entitled to access.” *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009). An individual thus “exceeds authorized access” only when she accesses information she is not otherwise permitted to access, regardless of the purpose for which she accesses the information. See *WEC Carolina*, 687 F.3d at 206; *Valle*, 807 F.3d at 527-28.

The question before this Court, then, is whether Appellant “exceed[ed] authorized access” when she accessed information that she was otherwise entitled to access but in a manner not permitted by the AUP.

The answer is no.

¹ “Entitle” is defined as “[t]o furnish with a right or claim to something.” See “entitle,” *The American Heritage Dictionary* (5th ed.), <https://www.ahdictionary.com/word/search.html?q=entitle>. As noted by the Ninth Circuit, for purposes of the CFAA, “[a]n equally or more sensible reading of ‘entitled’ is as a synonym for ‘authorized.’” *Nosal*, 676 F.3d at 857. “So read, ‘exceeds authorized access’ would refer to data or files on a computer that one is not authorized to access.” *Id.*

The legislative history is clear that the CFAA was designed to criminalize "hacking—the circumvention of technological access barriers[,]” see *Nosal*, 676 F.3d at 863, not violations of computer use restrictions. And the manner restriction at issue here is nothing more than a specific type of computer use restriction. Indeed, although there was a policy in place against the use of unauthorized programs to facilitate one’s access to the database, any such restriction did not alter the fact that Appellant was authorized to access the database. Such written, non-technical, policy-based restrictions on the manner in which individuals can obtain information they are otherwise authorized to access are restrictions on use, not access. Appellant’s conviction under Specification 13 of Charge II must therefore be reversed.

a) The CFAA was meant to target "hacking," not violations of computer use restrictions.

The CFAA "was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives[.]'" *Brekka*, 581 F.3d at 1130–31 (quoting H.R. Rep. 98–894, at 9, reprinted in 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984)). As both the Ninth Circuit and the lower court here recognized, relying on the CFAA’s legislative history, Congress’ purpose in enacting the CFAA was to target "hackers"

who “intentionally trespass[ed] into someone else’s computer files” and obtained information, including information on “how to break into that computer system.” *Nosal*, 676 F.3d at 858 (quoting S. Rep. No. 99-432, at 9, reprinted in 1986 U.S.C.C.A.N. 2479, 2487 (September 3, 1986)); see also 8 June 2012 Order, 6-7 (“[T]he statute is not meant to punish those who use a computer for an improper purpose or in violation of the governing terms of use, but rather the statute is designed to criminalize electronic trespassers and hackers.”) (citing *Int’l Ass’n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 495 (D. Md. 2005)).

As the Ninth Circuit further recognized, through targeting “hacking,” the CFAA’s purpose was “to punish . . . the circumvention of technological access barriers[.]” *Nosal*, 676 F.3d at 863. In other words, Congress intended to target those who circumvented code-based barriers to access—not those who violated written, policy-based computer use restrictions.² In

² The way for an employer or any other computer owner to indicate who is authorized and not authorized to access a computer system is to erect a technological, code-based access barrier—such as a username and password requirement—to allow authorized users in and keep unwanted individuals out. Without some barrier to entry, however, everyone is “authorized” to access data. See, e.g., *Pulte Homes, Inc. v. Laborer’s Int’l Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011) (public presumptively authorized to access “unprotected website”); *Craigslist, Inc. v. 3Taps, Inc.*, 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013) (“Craigslist II”) (making information website publicly available gives everyone “authorization” to view it under the CFAA). In other

this way, Congress sought to address a narrow problem, not create “a sweeping Internet-policing mandate.” *Id.* at 858; see also *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 932 (E.D. Va. 2010) (“The CFAA is a civil and criminal anti-hacking statute designed to prohibit the use of hacking techniques to gain unauthorized access to electronic data.”).

Numerous courts—including the three most recent federal circuit courts to address the issue—have interpreted the phrase “exceeds authorized access” to criminalize only the actions of authorized users who go beyond their authorization and access data they are not entitled to obtain at all, and not the actions of those who have authority to access data but who do so for a purpose that violates a contractual agreement or unilaterally-imposed use policy. See *Nosal*, 676 F.3d at 858; *WEC Carolina*, 687 F.3d at 199; *Valle*, 807 F.3d at 527–28. Though this scenario most often comes up in civil cases involving disputes between employers and employees—e.g., where an employee takes data for a purpose prohibited by the employer—the rationale of these decisions applies equally in criminal CFAA cases, such as *Nosal*, *Valle*, or this case. Indeed, courts “must interpret [a] statute consistently, whether [it] encounter[s] its application in a criminal or noncriminal context[.]” *Leocal v. Ashcroft*, 543 U.S.

words, the erection of a password barrier is what permits an employer or other computer owner to determine who has authorization to access a protected computer system or website.

1, 11, n.8 (2004). This rule applies to the CFAA, just as any other statute. See *WEC Carolina*, 687 F.3d at 204 (interpretation of CFAA “applies uniformly” in both civil and criminal cases).

Thus, the Ninth Circuit in *Brekka* (a civil case) noted that “[n]othing in the CFAA suggests that a defendant’s liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer,” such as violating an employer’s computer use policies. *Brekka*, 581 F.3d at 1135.

Three years later, the Ninth Circuit, sitting en banc in *Nosal* (a criminal case), affirmed a narrow construction of the phrase “exceeds authorized access” and rejected the argument that the bounds of an individual’s “authorized access” turned on use restrictions imposed by an employer. *Nosal*, 676 F.3d at 857. The Ninth Circuit explicitly stated its concern that interpreting the phrase “exceeds authorized access” to include violations of computer use policies “would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute.” *Id.* As the court noted, “[i]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose.” *Id.*

After *Nosal*, the Fourth Circuit in *WEC Carolina* (a civil case) narrowly interpreted the terms “without authorization” and “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.” *WEC Carolina*, 687 F.3d at 206. In rejecting a broad definition of the terms, the Fourth Circuit stated that it was “unwilling to contravene Congress’s intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy.” *Id.* at 207.

Three years later, the Second Circuit in *Valle* (a criminal case) joined the Fourth and Ninth Circuits in adopting a narrow interpretation of the phrase “exceeds authorized access” for purposes of the CFAA. 807 F.3d at 527–28. The district court had upheld the defendant’s CFAA conviction on the ground that the relevant policy stated that the database at issue “could only be accessed in the course of an officer’s official duties.” *Id.* at 513 (emphasis added). Although the policy included the word “access,” the Second Circuit reversed, recognizing that such purpose-based limits are de facto restrictions on use, regardless of the terminology employed. *Id.* at 528.

Ultimately, *Brekka*, *Nosal*, *WEC Carolina*, and *Valle*—and numerous other district courts³—narrowly interpreted the CFAA to not only consistently apply Congress’s intent to criminalize “hacking,” but also to avoid an unconstitutionally vague interpretation of the statute that would criminalize common, innocuous behavior. See, e.g., *Valle*, 807 F.3d at 527 (citing *Nosal*, 676 F.3d at 863).

As the lower court here acknowledged, some courts have broadly interpreted “without authorization” and “exceeds authorized access” to include acts of disloyal employees who

³ See, e.g., *Cloudpath Networks, Inc. v. SecureW2 B.V.*, ___ F. Supp. 3d ___, 2016 WL 153127, at *17 (D. Colo. Jan. 13, 2016); *Lane v. Brocq*, 2016 WL 1271051, at *10 (N.D. Ill., March 28, 2016); *Experian Marketing Solutions, Inc. v. Lehman*, 2015 WL 5714541, at *5 (W.D. Mich. Sept. 29, 2015); *Giles Const., LLC v. Tooele Inventory Solution, Inc.*, 2015 WL 3755863, at *3 (D. Utah Jun. 16, 2015); *Enhanced Recovery Co., LLC v. Frady*, 2015 WL 1470852, at *6-*7 (M.D. Fla. Mar. 31, 2015); *Cranell Inc. v. Pro Image Consultants Group, LLC*, 57 F. Supp. 3d 838, 845-46 (S.D. Ohio 2014); *Advanced Fluid Systems, Inc. v. Huber*, 28 F. Supp. 3d 306, 329 (M.D. Pa. 2014); *Dresser-Rand Co. v. Jones*, 957 F. Supp. 2d 610, 619 (E.D. Pa. 2013); *Power Equipment Maintenance, Inc. v. AIRCO Power Services, Inc.*, 953 F. Supp. 2d 1290, 1295 (S.D. Ga. 2013); *Lewis-Burke Associates, LLC v. Widder*, 725 F. Supp. 2d 187, 194 (D.D.C. 2010); *Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010); *Clarity Servs., Inc. v. Barney*, 698 F. Supp. 2d 1309, 1315 (M.D. Fla. 2010); *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 615 (M.D. Tenn. 2010); *Nat’l City Bank, N.A. v. Republic Mortgage Home Loans*, 2010 WL 959925, at *3 (W.D. Wash. Mar. 12, 2010); *Black & Decker, Inc. v. Smith*, 568 F. Supp. 2d 929, 934 (W.D. Tenn. 2008); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008); *Diamond Power Int’l., Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); *Int’l Ass’n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005).

misuse their access to corporate information. See, e.g., *United States v. John*, 597 F.3d 263, 272–73 (5th Cir. 2010); *Int’l Airport Ctrs. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582–84 (1st Cir. 2001); *United States v. Rodriguez*, 628 F.3d 1258, 1263–64 (11th Cir. 2010). But this broad interpretation of the CFAA has been explicitly rejected by the more recent decisions. See *Nosal*, 676 F.3d at 862–63 (rejecting *John*, *Citrin*, and *Rodriguez* for failing to “construe ambiguous criminal statutes narrowly so as to avoid ‘making criminal law in Congress’s stead’”) (quoting *United States v. Santos*, 553 U.S. 507, 514 (2008)); *WEC Carolina*, 687 F.3d at 206 (rejecting *Citrin* because it had “far-reaching effects unintended by Congress”); *Valle*, 807 F.3d at 527–28. As one district court noted, the courts that have broadly interpreted the CFAA “wrap the intent of the employees and use of the information into the CFAA despite the fact that the statute narrowly governs access, not use” and fail “to consider the broad consequences of incorporating intent into the definition of ‘authorization.’” *Dresser-Rand*, 957 F. Supp. 2d at 619.

This Court should adopt the reasoning of the Second, Fourth, and Ninth Circuits and explicitly reject the notion that violations of computer use restrictions—which, as outlined below, include written, policy-based restrictions regarding

“manner” of access—can result in federal criminal liability. Indeed, as *Nosal* instructs, CFAA prosecutions should be focused on “hacking—the circumvention of technological access barriers.” 676 F.3d at 863.

b) Written, policy-based restrictions on manner of access are restrictions on use.

The lower court acknowledged that many courts have concluded that employees are not liable under the CFAA for misappropriating confidential information in violation of computer use policies. See 8 June 2012 Order, 7-8. But it distinguished these cases by concluding that the manner restriction at issue here was a restriction on access, rather than on use. 18 July 2012 Order, 2. The court’s rationale is flawed in two critical respects.

First, the lower court erroneously found that “[r]estrictions on access to classified information are not limited to code based or technical restrictions on access” and “can arise from a variety of sources, to include regulations, user agreements, and command policies.” See *id.* While no federal court has explicitly ruled that the government is required to prove circumvention of a technological access barrier to establish CFAA liability, that is the inescapable conclusion of *Nosal*, *Brekka*, *WEC Carolina*, and *Valle* given the courts’ repeated discussion of the CFAA as an anti-hacking statute. See, e.g., *Nosal*, 676 F.3d at 863; *Brekka*, 581 F.3d at 1130 (“The act

was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives[.]'""); WEC Carolina, 687 F.3d at 201; Valle, 807 F.3d at 526. Indeed, implicit in these courts' decision to distinguish between "hacking" and authorized access is an understanding that the former requires defeating some technological access barrier. And *Brekka's* discussion of "authorization"—and how it is the actions of the employer who maintains a given computer system that determine whether a person is acting with or without authorization—is simply another way of stating that circumvention of a technological access barrier is necessary for purposes of the CFAA. See *Brekka*, 581 F.3d at 1135.⁴

⁴ The 1996 Senate Report cited by the lower court, which discussed an amendment to the CFAA, does not support a conclusion to the contrary. See S. Rep. No. 104-357, at 6 (1996). The report does not explicitly address whether access restrictions must be code-based. It is ambiguous at best about whether section 1030(a)(1), as amended, requires an insider to circumvent technological access restrictions in order to exceed authorized access. It also creates ambiguity about whether section 1030(a)(1) proscribes "access" to information versus "use" of computers—a question that has been affirmatively resolved by numerous federal courts and the lower court in this case. The cited text thus only creates ambiguity, rather than resolves it. This Court should therefore disregard both the cited text and the lower court's conclusions drawn from it. See *Milner v. Dep't of Navy*, 562 U.S. 562, 574 (2011) ("Legislative history, for those who take it into account, is meant to clear

Second, the court incorrectly concluded that restrictions on access “can include manner of access” and that use agreements “can also contain restrictions on access as well as use.” See 18 July 2012 Order, 2. Here, the lower court misconstrued the nature of not only the use restriction at issue in this case, but also of computer use agreements in general. The lower court was correct in characterizing the restriction at issue—which purportedly restricted Appellant’s ability to use unauthorized software (such as Wget) to access the NCD database⁵—as one on “manner” of access. But such a written, policy-based restriction governing *how* one accesses information that they are already authorized to access constitutes a limit on how they *use* their authorization. Such policy-based restrictions on manner of access are thus simply a form of use restriction. See *Koch Industries*, 2011 WL 1775765, at *8 (D. Utah May 9, 2011) (“[P]laintiff’s claim was really a claim that a user with authorized access had used the information in *an unwanted manner*, not a claim of unauthorized access or of exceeding authorized access.”) (citing *Cvent*, 739 F. Supp. 2d at 933) (emphasis added).

up ambiguity, not create it.”).

⁵ The written text of the AUP was not introduced into the record. But regardless of whether the policy was phrased in terms of use or access, the restriction limited how Appellant could *use* her authorization to access the database and was thus a *use* restriction.

To be sure, the fact that the program Appellant used to access the database was not “authorized” did not render her own authorization invalid. The restriction at issue governed not what information Appellant could access, but only how Appellant could use her authorization. It is thus a restriction on use—not on access—and it is therefore irrelevant for assessing whether she “exceeded authorized access” to the database for purposes of the CFAA.

That the manner restriction here may have been phrased in terms of “access” does not change the analysis. Indeed, numerous other courts have recognized that restrictions contained within computer use policies do not become access restrictions simply because they are phrased in terms of “access.” For example, the restriction in *Valle* used the word “access,” but the Second Circuit nevertheless threw out the defendant’s conviction, finding that the restriction was nevertheless a purpose-based use restriction. *See Valle*, 807 F.3d at 527-28.

Similarly, in *Craigslist, Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962 (N.D. Cal. 2013) (“*Craigslist I*”), the court found a website’s terms of use—which prohibited some uses of data by site visitors—to be “use” restrictions even though they were “framed in terms of ‘access[.]’” 942 F. Supp. 2d at 969. Because the restrictions “depend[ed] entirely on the accessor’s purpose,” the court concluded that the terms of use contained “only ‘use’

restrictions, not true 'access' restrictions[.]” *Id.* As the court stated in a later opinion in the same case, “simply denominating limitations as ‘access restrictions’ does not convert what is otherwise a use policy into an access restriction. . . . Thus, purported ‘de-authorizations’ buried in a website’s terms of service may turn out to be use restrictions in disguise.” *Craigslist II*, 964 F. Supp. 2d at 1185 (citations and internal quotations omitted).

Likewise, in *Wentworth-Douglass Hospital v. Young & Novis Professional Association*, 2012 WL 2522963, at *4 (D.N.H. June 29, 2012), the court rejected the plaintiff’s claim that the restriction at issue was an “access” restriction. According to the court, “the [plaintiff’s] policy prohibiting employees from accessing company data for the purpose of copying it to an external storage device is not an ‘access’ restriction; it is a limitation on the use to which an employee may put data that he or she is otherwise authorized to access.” *Id.* The court held that “simply denominating limitations as ‘access restrictions’ does not convert what is otherwise a use policy into an access restriction.” *Id.* The court further noted that the defendants did not “hack” computers or otherwise circumvent technological access barriers in order to access the data in question. *Id.*

Here, there is no question that Appellant was authorized to access the NCD database, and that she did not have to circumvent

any technological access barriers in order to access the data in question—with or without the Wget software. Although the AUP prohibited use of unauthorized software to facilitate one's authorized access, just as in *Wentworth-Douglass Hospital*, any such restriction governed only "the use to which [Appellant] may put data that [she was] otherwise authorized to access." See *id.*

The lower court distinguished *Wentworth-Douglass Hospital* on the ground that it did not involve classified information belonging to the U.S. government. See 18 July 2013 Order, at 6. But the fact that the information accessed was classified should have no bearing for purposes of assessing whether a restriction is one on use versus one on access. Indeed, the CFAA's definition of "unauthorized access" to classified materials is not distinguished from "unauthorized access" to any other type of information. Rather, the CFAA uses "without authorization or exceeding authorized access" language in its various provisions. Ultimately, "identical words used in different parts of the same statute are generally presumed to have the same meaning." *IBP, Inc. v. Alvarez*, 546 U.S. 21, 34 (2005). Thus, an interpretation of the phrase "exceeds authorized access" for purposes of § 1030(a)(1) would apply equally to § 1030(a)(2), which simply criminalizes unauthorized access or exceeding authorized access to a protected computer. And although access restrictions are often more stringent for classified information, what

constitutes an access restriction versus a use restriction for purposes of the CFAA cannot vary based on the type of information accessed.⁶ Written, non-technical restrictions on manner of access within computer use policies are restrictions on use, no matter what data is being accessed.

For purposes of CFAA liability, the facts of this case are thus analogous to the various disloyal employee cases cited by the lower court. See 8 June 12 2012 Order, 7-8. Indeed, as an Army employee, Appellant was subject to a database use policy comparable to the corporate policies at issue in those cases intended to limit the purposes for which employees could use corporate data. See *WEC Carolina*, 687 F.3d at 202 (“WEC instituted policies that prohibited using the information without authorization or downloading it to a personal computer.”); *Nosal*, 676 F.3d at 856 & n.1 (opening screen of proprietary database included warning: “This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only.”); *Valle*, 807 F.3d at 513 (per NYPD policy, “databases could only be accessed in the course of an officer’s official duties” and not for personal use). That this

⁶ This would create significant notice problems. Due process requires that the law be clear as to what actions constitute unauthorized access across all types of information. The CFAA is “a criminal statute”—not some mere use policy or handbook—and it thus “must give fair warning of the conduct that it makes a crime[.]” *Bouie v. City of Columbia*, 378 U.S. 347, 350 (1964).

case involves a government entity rather than a private employer, or that the restrictions at issue here may have been phrased in terms of manner of access, is irrelevant to whether Appellant violated the CFAA. This case, like the ones discussed above, involves an employer's attempt to control the manner in which or purpose for which authorized users access information that they are otherwise authorized to access. This restriction, like the restrictions in the cases discussed above, is a de facto restriction on use, not a restriction on access, and cannot be the basis for CFAA liability.

2. The Lower Court's Broad Reading of the CFAA Renders the Statute Unconstitutionally Vague.

The competing interpretations of the CFAA outlined above demonstrate that the statutory language presents a significant threat of unconstitutional vagueness. A criminal statute can be void for vagueness if it either (a) fails to provide fair notice of what is criminal, or (b) threatens arbitrary and discriminatory enforcement. *Skilling v. United States*, 561 U.S. 358, 412 (2010) (citing *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)). As a result, the Rule of Lenity calls for ambiguous criminal statutes—particularly those that also impose civil liability—to be interpreted narrowly in favor of the defendant. *Santos*, 553 U.S. at 514. The Rule of Lenity “ensures fair warning by so resolving ambiguity in a criminal statute as to apply [] only to conduct clearly covered.” *United States v.*

Lanier, 520 U.S. 259, 266 (1997). Critically, 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.” *Nosal*, 676 F.3d at 863.

These vagueness concerns were at the heart of the Second, Fourth, and Ninth Circuits’ decisions to limit CFAA liability to violations of access restrictions. See, e.g., *Valle*, 807 F.3d at 527–28; *WEC Carolina*, 687 F.3d at 204; *Nosal*, 676 F.3d at 862–64. Here, the lower court purportedly followed the reasoning of these courts, but pursuant to its mistaken approach of imposing CFAA liability based on a violation of what amounts to a use restriction, the CFAA could very well be invalidated as vague—both for failing to give adequate notice and for risking arbitrary enforcement.

a) Corporate policies do not provide sufficient notice of what conduct is prohibited.

Due process requires that criminal statutes provide ample notice of what conduct is prohibited. See *Connally v. Gen. Const. Co.*, 269 U.S. 385, 390 (1926). But basing criminal liability on policies instituted by an employer—be it the NYPD as in *Valle* or a private corporation as in *Nosal*—confers on employers the power to outlaw any conduct they wish without the clarity and specificity required of criminal law. “[A]llow[ing] criminal liability to turn on the vagaries of private polices that are

lengthy, opaque, subject to change and seldom read” creates “[s]ignificant notice problems[.]” *Nosal*, 676 F.3d at 860.

The Ninth Circuit in *Nosal* highlighted the central problem with basing CFAA liability on computer use policies: such liability would permit “private parties to manipulate their computer-use and personnel policies” so as to turn employer-employee and company-consumer relationships—relationships traditionally governed by tort and contract law—“into ones policed by the criminal law.” *Id.* This would grant employers the power to unilaterally “transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved.” *Id.* Indeed, the terms of computer use policies are often drafted to address concerns far beyond the CFAA’s anti-hacking purpose.

And because employers retain the right to modify their corporate policies or terms of use at any time without notice, “behavior that wasn’t criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever.” *Id.* at 862. This result “gives employees insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited.” Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 *Minn. L. Rev.* 1561, 1586 (2010).

Publicly-available computer use policies demonstrate the notice problems inherent in premising criminal liability on corporate use policies. One Internet and email use policy, for example, states that computer use restrictions include "but are not limited to" seven specific prohibitions, as well as "any other activities designated as prohibited by the agency."⁷ Such lack of specificity is exacerbated by the fact that employers often reserve the right to change policies at any time without advance notice.⁸ Attaching criminal punishment to breaches of such vague, boilerplate policies would make it impossible for employees to know what conduct is criminally punishable at any given time.

⁷ Virginia Dep't of Human Resource Management, Use of the Internet and Electronic Communications Systems, <http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/poll175useofinternet.pdf?sfvrsn=2>; see also Susan M. Heathfield, Internet and Email Policy, http://humanresources.about.com/od/policiesandsamples1/a/email_policy.htm (warning that "Internet use, on Company time, is authorized to conduct Company business only," and "[o]nly people appropriately authorized, for Company purposes, may use the Internet[.]").

⁸ See, e.g., Employee Handbook, <http://www.hrvillage.com/download/Employee-Handbook-Template.pdf> ("The policies stated in this handbook are subject to change at any time at the sole discretion of the Company."); Dartmouth College, Employment Policies and Procedures Manual, <http://www.dartmouth.edu/~hrs/policy> ("The policies are intended as guidelines only, and they may be modified, supplemented, or revoked at any time at the College's discretion.").

b) Basing CFAA liability on violations of use restrictions would permit capricious enforcement by prosecutors.

As the Supreme Court has stated, "if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them." *Grayned v. Rockford*, 408 U.S. 104, 108 (1972). "A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application." *Id.* at 108-09.

The lower court's decision permits arbitrary and discriminatory enforcement by expanding the scope of CFAA liability to cover millions of ordinary individuals who violate computer use restrictions every day via innocuous and ordinary—indeed, routine—online behaviors, such as sending personal email or checking the score of a baseball game on ESPN.com. See *Nosal*, 676 F.3d at 860. This sweeping interpretation creates the potential for draconian results not only in the context of employees who momentarily stray from their work duties, but also in the context of Internet users who unknowingly violate a website's terms of use. Through interpreting the CFAA in a way that would "criminalize a broad range of day-to-day activities," the lower court subjects employees and Internet users alike to prosecution at the whim of prosecutors, who can pick and choose which violations they wish to penalize. See *United States v.*

Kozminski, 487 U.S. 931, 949 (1988). Such broad statutory interpretation “delegate[s] to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as crimes’ and would ‘subject individuals to the risk of arbitrary or discriminatory prosecution and conviction.’” *Nosal*, 676 F.3d at 862 (citing *Kozminski*, 487 U.S. at 949). Here, by giving that much power to prosecutors, the lower court has “invit[ed] discriminatory and arbitrary enforcement.” *Id.*⁹

As the Supreme Court has noted, the Constitution “does not leave us at the mercy of *noblesse oblige*” by the government. *United States v. Stevens*, 559 U.S. 460, 480 (2010); see also *Nosal*, 676 F.3d at 862. Indeed, “[w]hile the Government might promise that it would not prosecute an individual for checking Facebook at work, we are not at liberty to take prosecutors at their word in such matters.” *Valle*, 807 F.3d at 528. As the Second Circuit held in rejecting the government’s broad interpretation of the CFAA in *Valle*, “[a] court should not uphold a highly problematic interpretation of a statute merely

⁹ This would be true even if the lower court’s decision applied only to computer use restrictions phrased in terms of access, such as the manner-based restriction on access at issue in this case or the purpose-based restriction on access at issue in *Valle*. See 807 F.3d at 513. Employers and website owners would simply start drafting all computer use restrictions to read as “access” restrictions—or “manner of access” restrictions—to preserve potential CFAA liability.

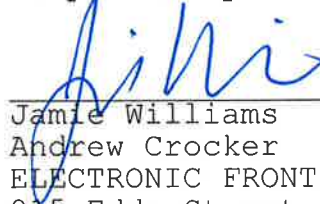
because the Government promises to use it responsibly." *Id.* at 528 (citing *Stevens*, 559 U.S. 460, 480 (2010)). In order to avoid fatal vagueness problems, the CFAA must be narrowly applied to only the behavior Congress clearly intended to criminalize: "hacking."

Conclusion

This Court should reverse Appellant's conviction under Specification 13 of Charge II.

Date: San Francisco, California
17 May 2016

Respectfully submitted,



Jamie Williams
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993
jamie@eff.org

*Counsel for Amici Curiae¹⁰
Electronic Frontier Foundation,
National Association of Criminal
Defense Lawyers, and Center for
Democracy & Technology*

¹⁰ Above-listed counsel are not admitted to practice before this Court and therefore request permission, pursuant to Rule 8(c) of the Court of Criminal Appeals Rules of Practice and Procedure, to appear *pro hac vice* for the limited purpose of submitting this amicus brief. Good cause exists to grant this request given the serious nature of the issues at stake in this case. Counsel are members in good standing of the bar in California and are admitted to practice before various federal courts.

CERTIFICATE OF FILING AND SERVICE

I certify that I have, this 17th day of May, 2016, filed and served the foregoing Unopposed Motion for Leave to File Brief of Amicus Curiae and its attached Brief of Amici Curiae Electronic Frontier Foundation, National Association of Criminal Defense Lawyers, and Center for Democracy & Technology in Support of Appellant via overnight courier, copies to the Clerk of Court, counsel for Appellee, CPT Christopher A. Clausen, counsel for Appellant, Nancy Hollander, and the Government Appellate Division at the following addresses, respectively:

U.S. Army Court of Criminal Appeals
Mr. Squires, Clerk of Court
9275 Gunston Road
Fort Belvoir, VA 22060-5546
Tel: (703) 693-1301

- and -

Capt. Judge Advocate Christopher A. Clausen
Appellate Government Counsel
Government Appellate Division, Branch III
U.S. Army Legal Services Agency
9275 Gunston Road, Room 2005
Fort Belvoir, VA 22060
Tel: (703) 693-0775
christopher.a.clausen2.mil@mail.mil

- and -

Nancy Hollander (counsel for Pfc. Manning)
Vincent Ward
Freedman Boyd Hollander Goldberg Urias & Ward P.A.
20 First Plaza, Suite 700
Albuquerque, NM 87102
Tel: (505) 244-7517
nh@fbdlaw.com

- and -

Capt. Judge Advocate Dave Hammond
Appellate Defense Counsel
U.S. Army Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, VA 22060
Tel: (703) 693-0716
james.d.hammond7@mil@mail.mil


Cynthia Dominguez