No. 10-10038

IN THE
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellant

v.

DAVID NOSAL,
Defendant-Appellee

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTICT OF CALIFORNIA

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION SUPPORTING THE APPELLEE AND URGING AFFIRMANCE

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

Attorney for *Amicus Curiae*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND LEGISLATIVE AUTHORITIES

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, makes the following disclosures:

1. *Amicus* is not publicly held corporations or other publicly held entities.

2. *Amicus* has no parent corporations.

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

/s/ Marcia Hofmann — September 14, 2010
Marcia Hofmann
Electronic Frontier Foundation

STATEMENT OF *AMICUS CURIAE*

Amicus is a non-profit public interest organization seeking to ensure the proper application of the Computer Fraud and Abuse Act and maintain 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 computer crime, 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 www.eff.org.

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

I. INTRODUCTION AND SUMMARY OF ARGUMENT

This case presents a simple question: when an employee accesses a company computer with permission, but for a purpose that the company has not authorized, has the employee "exceeded authorized access" for purposes of the Computer Fraud and Abuse Act? The answer is no. The plain language of the statute, its legislative history, and constitutional concerns require this Court to interpret the phrase "exceeds authorized access" narrowly to avoid turning millions of ordinary computer users into criminals.

The government alleges that defendant David Nosal induced three employees of his former employer who were authorized to access the firm's computer system to obtain information in a proprietary database and pass it along to Nosal, who used it to start a competing business. The government argues that since these actions breached corporate policies, they also violate the CFAA.

As this Court held just last year in *LVRC Holdings LLC v. Brekka*, 571 F.3d 1127, merely violating a duty of loyalty to an employer cannot and should not form the basis for criminal liability under the CFAA. This decision comports with a string of recent decisions from other courts rejecting overbroad applications of the statute. The government's arguments, in contrast, would make it a federal crime to breach the arbitrary and often confusing employment policies written by private parties. This result would not only greatly increase the scope of criminal liability, but also create legal uncertainty and the possibility of capricious and discriminatory enforcement by the government. The Court should not construe the CFAA this was to avoid rendering the statute unconstitutionally vague.

This Court must reject the government's attempt to broaden the CFAA beyond the scope that Congress has explicitly established, and affirm the district court's decision.

II. STATEMENT OF THE CASE

Defendant David Nosal was a high-level executive at Korn/Ferry International ("Korn/Ferry"), an executive search firm. ER 22-23. He left the firm in October 2004, and signed a separation agreement providing that he would not perform executive search services for a year in exchange for regular payments from Korn/Ferry. ER 23.

Nosal's co-defendant Becky Christian was also employed by Korn/Ferry. ER 23. The superseding indictment alleges that Christian and two other Korn/Ferry employees used their legitimate credentials to access information in one of Korn/Ferry's proprietary databases with the purpose of helping Nosal to create his own executive search firm. ER 26-34. Specifically, the government alleges that while still employed at Korn/Ferry, the employees used password-protected user accounts provided by the firm to log into its computer system and access the "Searcher" database, which contained information about executives and companies, and obtained source lists and "custom reports" for Nosal. ER 26-34. The government argues that the employees' authorization to access the database was prescribed in the following ways:

- Korn/Ferry employees were issued unique user names and then created passwords, "which were intended to be used by the Korn/Ferry employees only." ER 25; Gov't Brief 5.
- Upon logging in to the Korn/Ferry computer system, employees were shown the following notification:

  > This computer system and information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry system or information and to do so without the relevant authority can lead to disciplinary action or criminal prosecution[.]

  ER 25; Gov't Brief 5.
- All employees signed agreements providing that the information in

Korn/Ferry's computer system is the property of the firm, and use or disclosure of that information for purposes other than Korn/Ferry business is prohibited. ER 25; Gov't Brief 5.

- Korn/Ferry marked each Custom Report generated from the Searcher database "Korn/Ferry Proprietary and Confidential." ER 25; Gov't Brief 5.
- The government argues in its appellate brief — though does not allege in the superseding indictment — that Korn/Ferry's computer system would display the following pop-up banner before employees accessed the Custom Report feature of the Searcher: "[t]his product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only." Gov't Brief 5.

For the remainder of this brief, these notices and agreements will be collectively referred to as "corporate policies."

The government indicted Nosal and Christian on twenty counts, including trade secret theft, mail fraud and computer intrusion under 18 U.S.C. § 1030(a)(4), which prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value[.]" ER 22-39.

Nosal moved to dismiss the superseding indictment, arguing, *inter alia*, that counts 2-9 failed to state an offense under the CFAA. In an April 13, 2009 order, the district court denied Nosal's motion with respect to those counts. ER 40-54. Noting that there are two diverging lines of precedent on the question of whether an employee's authorization to access a company computer terminates when the employee violates her duty of loyalty to her employer, the court adopted the more expansive view and held it does. ER 46-49.

In September 2009, however, the Ninth Circuit rejected the expansive view

of the CFAA. In *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the Court limited the CFAA's reach in the employment context when it held that that an employee uses a company computer "without authorization" under the CFAA only where she "has not received permission to use that computer for any purpose . . . or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id*. at 1135. While *Brekka* did not expressly interpret the phrase "exceeds authorized access," the Court noted that the term "implies that an employee can violate employer-placed limits on accessing information stored on that computer and still have authorization to access that computer." *Id*.

Following the decision in *Brekka*, the district court reconsidered its earlier ruling and reversed itself, holding that no CFAA violation occurred when Christian and another employee accessed the Searcher database because they were at the time both employed by Korn/Ferry and had permission to access the database "in the form of valid, non-rescinded usernames and passwords." ER 1-13. The court further held that neither Korn/Ferry's employment agreements, nor express disclaimers on certain Searcher documents indicating that the accessed material was proprietary and confidential, nor notices generated by the computer system stating that the system and information therein were confidential altered the result. ER 10. Rather, "[a]n individual only "exceeds authorized access" if she has permission to access a portion of the computer system but uses that access to "obtain or alter information in the computer that [she] is not entitled so to obtain or alter." ER 10, citing 18 U.S.C. § 1030(e)(6). The court also noted that the government's argument raised rule of lenity concerns. ER 11. Accordingly, the court dismissed counts 2 and 4-7.[1] ER 11. The government now appeals.

[1] The court did not dismiss counts 3 or 8 because, while, they do not specify who accessed the Korn/Ferry system or whether the individual accessed parts of the system that he or she was not authorized to access, the government claims that it

III. ARGUMENT

A. The Computer Fraud And Abuse Act Does Not Prohibit Mere Violation Of Corporate Policies

Section 1030(a)(4) of the CFAA prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value[.]" The government concedes that this Court's holding in *Brekka* forecloses the argument that the Korn/Ferry employees accessed the firm's computer system "without authorization." Gov't Brief at 23. Thus, the only question before this Court is whether they "exceeded authorized access" by accessing information — which they were otherwise entitled to access — in violation of rules set forth in Korn/Ferry's corporate policies.

A straight-forward reading of the statutory definition of "exceeds authorized access" shows that they did not. The term is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6); *see also Brekka*, 581 F.3d at 1133 ("a person who 'exceeds authorized access' . . . has permission to access the computer, but accesses information on the computer that the person is not entitled to access"). Thus, while the CFAA's prohibition against accessing a protected computer "without authorization" covers outsiders who have no rights to the computer system, the prohibition against "exceed[ing] authorized access" is aimed at "insiders" who have some rights to access part of a computer system, but do not have rights to access or alter certain other files or information on that same system. As the government notes, the dictionary defines "entitle" as

---

will establish at trial that a Korn/Ferry employee logged into the system and Christian ran queries in the Searcher database without authorization, after her employment with Korn/Ferry ended. ER 11-12. Count 9 was not dismissed because the court found that the government properly alleged that another employee accessed Korn/Ferry's computer system "without authorization," since his employment there had ended at the time of access. ER 12-13.

"to furnish with a right." Gov't Brief at 15. The Korn/Ferry employees were furnished with a right to access information in the Searcher database in the form of log-in credentials.

There is no question that the employees were authorized to access the information using their log-in credentials. But the government argues that the employees "exceeded authorized access" when they "access[ed] and obtain[ed] information for a non-business purpose, in violation of Korn Ferry's corporate polices." Gov't Brief at 25-26. In other words, the government believes that criminal liability attaches when an employee has a state of mind that violates a corporate policy at the time she accesses information that she is otherwise entitled to access. This is not, however, what the statute says. When Korn/Ferry gave its employees credentials to access its computer system, it gave them the "authorization" to access that system and obtain the information that the credentials allowed them to access.

The plain language of the statute resolves this case. Even if it did not, however, the legislative history of the law confirms in no uncertain terms that the government's argument that employee purpose can negate "authorization" is wrong. In the 1986 amendments to the CFAA, Congress substituted the phrase "exceeds unauthorized access" for the phrase "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend." S. Rep. No. 99-432 at 9 (1986). The purpose of this amendment was to "eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend[.]'" *Id*. at 21. This effectively "remove[d] from the sweep of the statute one of the murkier grounds of liability, under which . . . access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed [] authorization." *Id*. Thus, Congress expressly amended the statute to remove the very "murky" ground for liability that the

government now urges the Court to accept.

Most of the recent cases interpreting the CFAA align with this plain congressional intent, holding that if a user is authorized to access a computer, then doing so is not criminal, even if that access violates a contractual agreement or unilaterally imposed policy.

The most important of these cases is *Brekka,* 581 F.3d 1127, which also arose in an employment context. In *Brekka*, the defendant was a marketing contractor for a residential treatment center for addicts. While so employed, and during negotiations to take an ownership interest in the facility, he emailed several of the facilities' files to himself. *Id.* at 1129-30. Subsequently, after the talks had terminated unsuccessfully and the defendant was no longer working for the facility, he used his log-in credentials to access the center's website statistics system. *Id.* at 1130. The company discovered his access, disabled the account and sued the defendant, alleging that he violated 18 U.S.C. §§ 1030(a)(2) and (a)(4) by emailing files to himself for competitive purposes and for accessing the statistics website. *Id.* This Court upheld summary judgment in favor of the defendant, finding that "a person who 'exceeds authorized access' . . . has permission to access the computer, but accesses information on the computer that the person is not entitled to access." *Id*. at 1133. Significantly, the Court found that "when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer *even if the employee violates those limitations*." *Id*. at 1133 (emphasis added). In other words, "[a] person uses a computer 'without authorization' under [section 1030(a)(4) only] when the person has not received the permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id*. at 1135.

The plaintiff in *Brekka* had pointed to the Seventh Circuit case *International*

Airport Centers, LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006), arguing that an employee can lose authorization to use a company computer when the employee resolves to act contrary to the employer's interest. The Ninth Circuit explicitly rejected that interpretation because section 1030 is a criminal statute that must have limited reach and clear parameters under the rule of lenity and to comply with the void for vagueness doctrine. *Brekka*, 581 F. 3d at 1134, citing *United States v. Carr*, 513 F.3d 1164, 1168 (9th Cir. 2008).[2]

Other courts have reached the same conclusion as this Court. In *Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479 (D. Md. 2005), the plaintiff argued that the defendant, a union officer, exceeded her authorization to use the union computer when she violated the terms of use to access a membership list with the purpose to send it to a rival union, and not for legitimate union business. *Id*. at 495-96. The defendant had signed an agreement promising that she would not access union computers "contrary to the policies and procedures of the [union] Constitution." *Id*. The court rejected the application of section 1030, holding that even if the defendant breached a contract, that breaking a promise not to use information stored on union computers in a particular way did not mean her access to that information was unauthorized or criminal:

> Thus, to the extent that Werner-Masuda may have breached the Registration Agreement by using the information obtained for purposes contrary to the policies established by the [union] Constitution, it does not follow, as a matter of law, that she was not authorized to access the information, or that she did so in excess of her authorization in violation of the [Stored Communications Act] or

---

[2] In addition, *Citrin* interpreted a subsection of the CFAA that prohibits "knowingly caus[ing] the transmission of a program, information, code or command, and as a result of such conduct, *intentionally causes damage without authorization*, to a protected computer." 18 U.S.C. § 1030(a)(4)(A)(i) (emphasis added). This provision is not violated by merely accessing a computer without authorization or in excess of authorization, as section 1030(a)(4) is. *Shamrock Foods v. Gast*, 535 F. Supp. 2d 962, 967 n.1 (D. Ariz. 2008).

> the CFAA. . . . Although Plaintiff may characterize it as so, the gravamen of its complaint is not so much that Werner-Masuda improperly accessed the information contained in VLodge, but rather what she did with the information once she obtained it. . . . Nor do [the] terms [of the Stored Communications Act and the CFAA] proscribe authorized access for unauthorized or illegitimate purposes.

Id. at 499 (citations omitted).[3]

Subsequent cases have followed the reasoning of *Werner-Masuda* based on either plain language or legislative history. In *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 2007), the court rejected a CFAA claim against an employee who violated an employment agreement by using his access to his employer's computer system to steal data for a competitor. The defendant had transferred information from password-protected computer drives to his new employer while still employed with the former company, which violated a confidentiality agreement. *Id.* at 1327-31. Identifying the narrower interpretation of "exceeding authorized access" as "the more reasoned view," the court held that "a violation for accessing 'without authorization' occurs only where initial access is not permitted. And a violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted." *Id*. at 1343.

In *Shamrock Foods v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008), the court

---

[3] The *Werner-Masuda* court also considered whether the defendant's actions had violated the Stored Communications Act, 18 U.S.C. § 2701(a) ("SCA"). It found that the SCA "prohibit[s] only unauthorized access and not the misappropriation or disclosure of information." It continued: "there is no violation of section 2701 for a person with authorized access to the database no matter how malicious or larcenous his intended use of that access." (citing *Educ'al Testing Service v. Stanley H. Kaplan, Educ'al Ctr., Ltd*., 965 F. Supp. 731, 740 (D. Md. 1997) ("[I]t appears evident that the sort of trespasses to which the [SCA] applies are those in which the trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way"). *Werner-Masuda,* 390 F. Supp. 2d at 496.

relied on *Davidson* and *Werner-Masuda* to hold that the defendant did not access the information at issue "without authorization" or in a manner that "exceed[ed] authorized access." *Id.* at 968. The defendant had an employee account on the computer he used at the company where he was employed, and was permitted to view the specific files he allegedly emailed to himself. The court held that the CFAA did not apply, even though the emailing was for the improper purpose of benefiting himself and a rival company in violation of the defendant's confidentiality agreement.[4]

While the majority of the cases support the *Brekka* analysis, the Fifth Circuit recently held in *United States v. John* that a bank employee exceeded authorized access to the bank's computers when, contrary to corporate policy, she accessed information in customer accounts and gave it to another person, who used it to commit fraud. 597 F.3d 263 (5th Cir. 2010). *Amicus* respectfully submits that this decision was in error. In that case, the court found that "[a]n authorized computer

---

[4] For additional cases rejecting criminal liability under the CFAA when the defendant had authorization to access the system or data in question, but misused that authority, see *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006) and *Brett Senior & Assocs., P.C. v. Fitzgerald*, 2007 WL 2043377 (E.D. Pa. July 13, 2007).

The cases discussed above contrast with and reject earlier decisions, most importantly *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000). In *Shurgard*, the court denied a motion to dismiss a CFAA claim brought by an employee who took employer information from the computer system with him to his next job. *Id.* at 1129. The court relied on the Restatement (Second) of Agency, § 112 (1958), to hold that when the plaintiff's former employees accepted new jobs with the defendant, the employees "lost their authorization and were 'without authorization' [under the CFAA] when they allegedly obtained and sent [the plaintiff's] proprietary information to the defendant via e-mail." *Shurgard*, 119 F. Supp. 2d at 1125. The *Shurgard* approach has troubling and potentially unconstitutional results, such as criminalizing employee disloyalty or other transgressions against the mere preferences of a private party.

user has 'reason to know' that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme." *Id*. at 273. But John's employer had given her credentials to access the bank's system, thus authorizing her to access the information within it. She may well have violated various other laws for conspiring to defraud the bank's customers, but she did not violate the CFAA.

In sum, the better-reasoned cases in the Ninth Circuit and elsewhere explicitly reject the notion that a violation of a private agreement or corporate policy should result in federal criminal liability.

B. A Broad Reading of The Computer Fraud and Abuse Act Risks Rendering The Statute Unconstitutionally Vague

The Court should be particularly careful not to adopt a broad interpretation of the phrase "exceeds authorized access" because the scope of the CFAA is already vast. Since first enacted in 1984, the federal computer crime law has been expanded by Congress several separate times. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1563-71 (2010) (describing in detail the expansion of the CFAA over the years). While originally a narrow, carefully prescribed statute, the law has grown unwieldy and could easily be interpreted in a manner that makes it unconstitutionally vague.

Congress has expanded two provisions of the CFAA over the years that have given the law an incredible sweep. The first is the definition of "protected computer." The second is section 1030(a)(2), which prohibits unauthorized access or exceeding authorized access to a protected computer. While the superseding indictment alleges violations of section 1030(a)(4), which prohibits unauthorized access or exceeding authorized access with intent to defraud, rather than section 1030(a)(2), both provisions prohibit access to a computer without authorization or exceeding authorization. The effect of those phrases in section 1030(a)(2) is therefore appropriate for consideration here, since section 1030(a)(4) contains

identical terms that should be interpreted in an identical manner by the courts.

1. Protected Computers

The first incarnation of the federal computer crime law, enacted in 1984, was a narrow statute intended to criminalize unauthorized access to computers to obtain national security secrets, to obtain personal financial and consumer credit information, and to hack into government computers. Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190, *codified at* 18 U.S.C. § 1030(a)(1)-(3). Congress added three new prohibitions two years later when it passed the Computer Fraud and Abuse Act of 1986. Pub. L. No. 99-474, 100 Stat. 1213. The 1986 amendments criminalized unauthorized access to a computer with intent to defraud; unauthorized access to a computer and altering, damaging, or destroying information and causing a certain amount of damage; and trafficking in passwords. 18 U.S.C. § 1030(a)(4)-(6) (Supp. IV 1987). The first two crimes were limited to those affecting "Federal interest" computers, which include computers used by the United States government or financial institutions, or "which is one of two or computers used in committing the offense, not all of which are located in the same State[.]" 18 U.S.C. § 1030(e)(2) (Supp. IV 1987).

In 1996, Congress significantly expanded the CFAA when it passed the National Information Infrastructure Protection Act of 1996. Critically, these amendments replaced the statutory definition of "Federal interest" computer with "protected computer," defined to include any computer used by the United States government or financial institutions, or "which is used in interstate or foreign commerce or communication[.]" 18 U.S.C. § 1030(e)(2) (Supp. II 1996). As George Washington University Professor Orin Kerr has noted, this change resulted in a massive expansion of the law: "Because every computer connected to the Internet is used in interstate commerce or communication, it seems that every computer connected to the Internet is a 'protected computer' covered by [the CFAA]." *Vagueness Challenges*, 94 Minn. L. Rev. at 1568.

The definition of "protected computer" was expanded again by the USA PATRIOT Act of 2001 to include computers outside the United States "that [are] used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B) (Supp. II 2004). This change effectively ensured that the CFAA applied to as many foreign computers as the Commerce Clause could reach, in addition to the huge number of U.S. computers already covered by the law. Kerr, *Vagueness Challenges*, 94 Minn. L. Rev. at 1568.

The Former Vice President Protection Act further extended the definition of "protected computer" in 2008. Pub. L. No. 110-326, 122 Stat. 3560. The definition now includes not just computers "used in interstate or foreign commerce or communication," but computers "used in *or affecting* interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2) (West 2000 & Supp. 2009) (emphasis added). The practical effect of this seemingly small change allows the CFAA to reach computers as far as the Commerce Clause can extend. Kerr, *Vagueness Challenges*, 94 Minn. L. Rev. at 1570. As Kerr explains:

> Because the definition now applies to both computers in the United States and abroad, that are used in or affecting interstate commerce or communication, every computer around the world that can be regulated under the Commerce Clause is a "protected computer" covered by 18 U.S.C. 1030. This does not merely cover computers connected to the Internet that are actually "used" in interstate commerce. Instead, it applies to all computers, period, so long as the federal government has the power to regulate them.

Id. at 1570-71.

2. Section 1030(a)(2)

As noted above, the federal computer crime statute originally prohibited unauthorized access to financial records from financial institutions, card institutions, or consumer reporting agencies. Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190, *codified at* 18 U.S.C. § 1030(1)-(3). The

1996 amendments dramatically expanded section 1030(a)(2) — which had originally prohibited unauthorized access to financial records from financial institutions, card institutions, or consumer reporting agencies — to prohibit unauthorized access to any information of any sort, so long as the conduct involved an interstate or foreign communication. 18 U.S.C. § 1030(a)(2)(C) (Supp. IV 1987).

In 2008, Congress again expanded section 1030(a)(2) by removing the requirement of an interstate communication. Pub. L. No. 110-326, § 103, 122 Stat. at 3561, *codified at* 18 U.S.C. § 1030(a)(2) (West 2000 & Supp. 2009). As a result, the provision now prohibits any unauthorized access to any protected computer that retrieves any information. "The statute essentially makes it a federal crime to access without authorization or exceed authorized access to any computer at all anywhere in the world. As a result, the meaning of unauthorized access determines the scope of the statute." Kerr, *Vagueness Challenges*, 94 Minn. L. Rev. at 1577. If this language is interpreted broadly, as the government urges, the scope of the statute will be virtually limitless.

C. The Court Must Interpret The Computer Fraud And Abuse Act Narrowly To Ensure That It Does Not Become Unconstitutionally Vague

Given the CFAA's already broad scope, imposing criminal liability under section 1030 whenever an employee oversteps corporate policies threatens to create constitutional vagueness problems. As the Supreme Court has observed, courts must adopt a narrow construction of a criminal statute to avoid vagueness. *See United States v. Skilling*, 130 S. Ct. 2896, 2927-28 (2010); *Kolender* v. *Lawson*, 461 U.S. 352, 357 (1983). Criminal punishment cannot be based on the vagaries of privately created, frequently unread, generally lengthy policies that may be altered without notice. Such documents fail to put employees on adequate notice of what conduct is criminally prohibited, and enables the government to enforce the law in an arbitrary and discriminatory manner.

A plurality of the Supreme Court has specified that "[v]agueness may invalidate a criminal law for either of two independent reasons. First, it may fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits; second, it may authorize and even encourage arbitrary and discriminatory enforcement." *Chicago v. Morales*, 527 U.S. 41, 56 (1999) (Stevens, J., plurality opinion). In the Ninth Circuit, "[t]o survive vagueness review, a statute must '(1) define the offense with sufficient definiteness that ordinary people can understand what conduct is prohibited; and (2) establish standards to permit police to enforce the law in a non-arbitrary, non-discriminatory manner.'" *United States v. Sutcliffe*, 505 F.3d 944, 953 (9th Cir. 2007) (quoting *Nunez v. City of San Diego*, 114 F.3d 935, 940 (9th Cir. 1997)). Unless construed narrowly, the CFAA could be invalidated for both of these reasons.

1. Corporate Policies Do Not Provide Sufficient Notice Of What Conduct Is Prohibited

Basing criminal liability on mere notice from an employer confers the power to outlaw any speech or conduct the employer wishes, and to do so without the sufficient clarity and specificity required of criminal law. This is especially troubling here because the government seeks to enforce policies aimed not at behavior, but at purpose and intent. That result is unacceptable regardless of whether the employer's objection is lodged in a contractual agreement or a corporate policy. The government's theory:

> gives employees insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited. The key consideration seems to be motive, but the employee has no way to determine what motives are illicit — and in the case of mixed motives, what proportion are illicit. Is use of an employer's computer for personal reasons always prohibited? Sometimes prohibited? If sometimes, when? And if some amount of personal use is permitted, where is the line? If use of an employer's computer directly contrary to the employer's interest is required, how contrary is directly contrary? Is mere waste of the employee's time enough? The cases generally deal with the dramatic facts of an employee who accessed a sensitive and valuable database to gather data that could be used to

> establish a competing company. But how sensitive does the database need to be? How valuable does the data need to be? The agency theory of liability under the CFAA does not appear to answer these questions.

Kerr, *Vagueness Challenges*, 94 Minn. L. Rev. at 1586. Under the government's interpretation of section 1030, the statute's essential meaning depends on the existence and clarity of employment policies that are aimed at employees' intentions rather than actions, and which have been drafted for reasons that have nothing to do with preventing the sort of unauthorized hacking, misuse, trespass or theft of private data with which the computer crime law is properly concerned.

Existing corporate Internet policies demonstrate the problem. One sample Internet and email usage policy, for example, warns that "Internet use, on Company time, is authorized to conduct Company business only," and "Only people appropriately authorized, for Company purposes, may use the Internet[.]"[5] Another policy that applies to all of Virginia's state government employees provides, "Certain activities are prohibited when using the Internet or electronic communications. These include, but are not limited to" seven specific prohibitions, as well as "any other activities designated as prohibited by the agency."[6] A policy's lack of specificity is often made worse by the fact that employers may reserve the right to change policies at any time, and not necessarily with advance notice.[7]

---

[5] Susan M. Heathfield, Internet and Email Policy, http://humanresources.about.com/od/policiesandsamples1/a/email_policy.htm (last visited Sept. 13, 2010).

[6] Virginia Dep't of Human Resource Management, Use of the Internet and Electronic Communications Systems, http://www.dhrm.state.va.us/hrpolicy/web/pol1_75.html (last visited Sept. 13, 2010).

[7] *See, e.g.*, Employee Handbook — Policies and Procedures, http://www.hrvillage.com/PandP/all.htm (last visited Sept. 13, 2010) ("The policies stated in this handbook are subject to change at any time at the sole discretion of the Company. From time to time, you may receive updated information regarding

Attaching criminal punishment to the breach of these vague, boilerplate policies would make it impossible for employees to know what conduct is criminally punishable at any given time.

2. If Accepted by the Court, the Government's Position Would Give Prosecutors Great Discretion to Arbitrarily and Discriminatorily Enforce Criminal Law

The government's interpretation of the CFAA would also render the law unconstitutionally vague because it would permit capricious enforcement. "[I]f arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them. 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." *Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972).

If the government's proposed construction of the CFAA is correct, millions of otherwise innocent employees commit frequent criminal violations of the law through ordinary — indeed routine — online behavior. As Kerr has noted:

> Employee use of computers tracks employee attention spans. Attention wanders, and our computer use wanders with it. We think, therefore we Google. As a result, it is rare, if not inconceivable, for every keystroke to be clearly and strictly in the course of furthering an employment relationship. The best employee in a larger company might spend thirty minutes writing up a report, then spend one minute checking personal e-mail and twenty seconds to check the weather to see if the baseball game after work might be rained out. He might then spend ten more minutes working on the report followed by two minutes to check the online news. Over the course of the day, he might use the computer for primarily personal reasons dozens or even hundreds of times.

Vagueness Challenges, 94 Minn. L. Rev. at 1585. Basing criminal liability on privately written corporate policies and agreements subjects employees to

---

any changes in policy."); Dartmouth College, Employment Policies and Procedures Manual, http://www.dartmouth.edu/~hrs/policy (last visited Sept. 13, 2010) ("The policies are intended as guidelines only, and they may be modified, supplemented, or revoked at any time at the College's discretion.").

prosecution at the whim of the government, which can pick and choose which violations it wishes to penalize. It does not matter that law enforcement might choose not to bring these cases. The inability of a reader to distinguish in a meaningful and principled way between innocent and criminal computer usage is the constitutional harm. *Humanitarian Law Project v. Mukasey*, 509 F.3d 1122, 1133 (9th Cir. 2007).

In the government's view, if a company's corporate policy says that work computer systems may be used only for legitimate company business — as Korn/Ferry's agreements do — and a worker looks at the website of her son's school to see whether a blizzard has caused classes to be cancelled that afternoon, she commits a computer crime. If she takes two minutes to check the balance of her bank account, email her spouse, or consult a bus schedule to make sure that she doesn't miss an appointment with her dentist, she violates the law. Even an employee who uses her company computer to order dinner delivery so that she can continue working on an important project through the evening risks criminal sanctions. Nearly any employer could choose to sue any employee — and the government could choose to prosecute virtually any worker — under this limitless standard.

This problem is not exclusive to employer policies unilaterally imposed upon workers. In other cases, the government has argued that an Internet user's breach of a website's terms of service should also violate the CFAA. *United States v. Lowson*, No. 10-cr-00144 (D. N.J. filed Feb. 23, 2010); *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (holding that a breach of MySpace's terms of use does not violate the CFAA). This expansive reading of the statute could turn millions of Internet users into criminals for typical, everyday Internet activity. For example, Google bars use of its services by minors — probably to protect itself against liability and to try to ensure its terms are binding in the event of a litigated

dispute.[8] Surely the company does not mean — or imagine — that tens of millions of minors will use its search engine or other services only at the risk of criminal liability.

Similarly, YouTube's Community Guidelines, expressly incorporated into the site's terms of use, prohibit posting videos that show "bad stuff." YouTube Community Guidelines, http://www.youtube.com/t/community_guidelines (last visited Sept. 13, 2010). Uploading "bad stuff" would not only violate YouTube's terms of service, but under the government's theory also constitute access without permission to the site. Surely YouTube did not draft the "bad stuff" prohibition with criminal liability in mind. Whatever the validity of holding such contracts enforceable for purposes of contract law,[9] the terms cannot define the line between lawful conduct and criminal violations.

The popular social networking service Facebook has terms of use that are also probably routinely violated. For instance, Facebook's terms of use provide:

- You will not provide any false personal information on Facebook.
- You will keep your contact information accurate and up-to-date.
- You will not share your password . . . [or] let anyone else access your

---

[8] Google Terms of Service § 2.3, http://www.google.com/accounts/TOS (last visited Sept. 13, 2010) ("You may not use the Services and may not accept the Terms if (a) you are not of legal age to form a binding contract with Google, or (b) you are a person barred from receiving the Services under the laws of the United States or other countries including the country in which you are resident or from which you use the Services.").

[9] *See* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 465, 475-76 (2006) (observing that in civil cases "in today's electronic environment, the requirement of assent has withered to the point where a majority of courts now reject any requirement that a party take any action at all demonstrating agreement to *or even awareness of terms* in order to be bound by those terms.") (emphasis added). This lax approach simply cannot provide "fair notice" in the criminal context.

account[.][10]

Under the government's theory, if a user shaves a few years off of her age in her profile information, or asserts that she is single when she is in fact married, or seeks to obfuscate her current physical location, hometown or educational history for any number of legitimate reasons, she violates federal computer crime law. And if a user changes jobs or moves to another city, she must immediately inform Facebook or run the risk that her continued use of the site could lead to criminal sanctions. Moreover, a politician or other high-profile user who communicates through Facebook with the general public violates the terms of use if he delegates administrative authority to employees or volunteers to maintain his page. *See, e.g.*, Barack Obama's Facebook Page, http://www.facebook.com/barackobama (last visited Sept. 13, 2010) (prominently noting that the page is "run by Organizing for America, the grassroots organization for President Obama's agenda for change.").

Even the remote possibility of enforcing private parties' preferences with criminal law puts immense coercive power behind corporate policies that may be contrary to the interests of employees and the public. Many of these polices contain terms that are vague, arbitrary or even fanciful. They are not written by their drafters with the precision and care that would be expected — indeed required — of operative provisions in a criminal statute. Nor are such terms necessarily written with the interests of society in mind.

To avoid fatal vagueness problems, the CFAA must be limited to clear, proper purposes consistent with the statute's goals, and not whatever commercial or personal purpose motivates a company to draft a policy in a certain way. For this reason, the long of cases ending with *Brekka* correctly rejected the approach the government urges the Court to adopt now.

---

[10] Facebook Statement of Rights and Responsibilities § 2, http://www.facebook.com/terms.php (last visited Sept. 13, 2010).

IV. CONCLUSION

The district court's decision must be affirmed. Any other result is inconsistent with the plain language of the statute and legislative history, and may well render section 1030 unconstitutional. Such an outcome will leave employees unsure what conduct might be criminal and will almost certainly result in increased exercise of prosecutorial discretion under an already worrisomely broad statute.

Date: September 14, 2010

By: /s/ Marcia Hofmann

MARCIA HOFMANN
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Attorney for *Amicus Curiae*

CERTIFICATE OF COMPLIANCE

This brief has been prepared in 14-point Times New Roman font. This brief contains 6,743 words and complies with the 7,000 word limitations pursuant to Rule 32.

By: /s/ Marcia Hofmann
MARCIA HOFMANN