IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

U N I T E D S T A T E S	)	
	)	**DEFENSE MOTION TO**
v.	)	**DISMISS FOR FAILURE TO**
	)	**STATE AN OFFENSE:**
	)	**SPECIFICATIONS 13 AND 14**
MANNING, Bradley E., PFC	)	**OF CHARGE II**
U.S. Army, xxx-xx-9504	)	
Headquarters and Headquarters Company, U.S.	)	
Army Garrison, Joint Base Myer-Henderson Hall,	)	DATED: 10 May 2012
Fort Myer, VA 22211	)	

RELIEF SOUGHT

1. PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 907(b)(1)(B), requests this Court to dismiss Specifications 13 and 14 of Charge II because the Government has failed to allege that PFC Manning's alleged conduct exceeded authorized access within the meaning of 18 U.S.C. Section 1030(a)(1).

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. The Defense, as the moving party, bears the burden of this motion by a preponderance of the evidence pursuant to R.C.M. 905(c)(1)-(2)(A). "A charge or specification shall be dismissed at any stage of the proceedings if: (A) [t]he court-martial lacks jurisdiction to try the accused for the offense; or (B) [t]he specification fails to state an offense." R.C.M. 907(b)(1).

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of conduct prejudicial to good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010).

4. In Specification 13 of Charge II, the Government pleads that PFC Manning

> did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, having knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer, and by

> means of such conduct having obtained . . . more than seventy-five classified United States Department of State cables, willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1)[.]

Charge Sheet (attached), Specification 13. Specification 14 of the same charge alleges that PFC Manning

> did, at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 18 February 2010, having knowingly exceeded authorized access on a Secret Internet Protocol Router Network Computer, and by means of such conduct having obtained . . . a classified Department of State cable titled "Reykjavik-13", willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1)[.]

Id., Specification 14. In its Bill of Particulars, the Defense asked the Government to specify how exactly it alleges that PFC Manning exceeded authorized access. The Government resisted providing these particulars. However, during the motions argument, CPT Morrow revealed the Government's position on how PFC Manning is alleged to have exceeded authorized access:

> MJ: Okay. Government, do you have a theory of a means by which he knowingly exceeded the unauthorized [sic] access?
>
> ATC1: The means?
>
> MJ: Yes.
>
> ATC1: Your Honor, the government would maintain that PFC Manning had a user name and a password to a SIPRNET computer while deployed. On certain occasions when he accessed that computer for certain, you know, to obtain these documents, he was exceeding authorized access. I can't – there is no means. I mean, there is no – I don't think it's – a mystery how he got onto the computer. I think Mr. Coombs is focusing on the [inaudible] diplomacy aspect of it when the focus should be on when he access [sic] the computer to do certain things.
>
> MJ: So your means is the fact that he accessed the computer to do certain things?
>
> ATC1: Yes, ma'am.
>
> MJ: All right. Are those things that he did part of the investigation or he –

ATC1: They are part of the specification, Your Honor. Obtaining these cables and transmitting to Wikileaks.

Oral Argument, Unauthenticated Transcript, 23 February 2012, pp. 71-72 [hereinafter Oral Argument, Unauthenticated Transcript].

WITNESSES/EVIDENCE

5. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the following evidence in support of the Defense's motion:

a. Charge Sheet (attached);

b. Oral Argument, Unauthenticated Transcript, 23 February 2012.

LEGAL AUTHORITY AND ARGUMENT

6. To state an offense under 18 U.S.C. Section 1030(a)(1), the Government must allege that the accused either knowingly accessed a computer without authorization or that he knowingly exceeded authorized access in accessing the information in question. The Government in this case has alleged that PFC Manning knowingly exceeded his authorized access when, despite being authorized to use the computer, he accessed certain information for an improper purpose and/or in violation of the governing terms of use, and disclosed the information to a person not authorized to receive it.

7. The plain language of Section 1030(e)(6) clearly indicates that a person exceeds authorized access when he or she uses authorized access to a computer to obtain or alter information in the computer that he or she is not entitled to obtain or alter. 18 U.S.C. § 1030(e)(6). Neither Section 1030(e)(6) nor Section 1030(a)(1) gives any indication that an accused's purpose in accessing the computer or the information in question is in any way relevant to the "exceeding authorized access" inquiry. *See id.* § 1030(a)(1), (e)(6). It is clear from the plain language of Section 1030(a)(1) that PFC Manning did not exceed authorized access within the meaning of the statute. PFC Manning had full authority to access the government computer(s) at issue and at no time did he obtain or alter information that he was not entitled to obtain or alter.

8. The essence of the Government's theory is either: a) that PFC Manning exceeded authorized access when he allegedly accessed information for an improper purpose, *viz.*, to give the information to someone not authorized to receive it; or b) that PFC Manning exceeded authorized access when he allegedly accessed, stored and disclosed information in contravention of the Army's Acceptable Use Policy (AUP).[1] Either way, the Government fails to state an

[1] This latter theory was presented by the Government at the Article 32 hearing.

offense under Section 1030(a)(1).[2] Under Section 1030(a)(1), an accused's purpose in accessing the computer is irrelevant, as is the question of whether the accused violated the employer's terms of use. The inquiry under Section 1030(a)(1) is strictly limited to whether the accused had authority to access the information accessed. Other sections of federal criminal law or the UCMJ may criminalize PFC Manning's alleged improper storing or dissemination of information – but not Section 1030(a)(1).

9. Additionally, interpreting the term "exceeds authorized access" to include instances where a person accesses information for an improper purpose or where a person violates the terms of use of that access poses serious constitutional concerns for at least one provision of the statute.[3] Therefore, this expansive interpretation must be rejected.

10. Because the Government has failed to allege that PFC Manning "exceeded authorized access" within the meaning of Section 1030(a)(1), the charge should be dismissed for failure to state an offense.

A. Under the Plain Language of 18 U.S.C. Section 1030(a)(1), PFC Manning Did Not Exceed His Authorized Access

11. As outlined in *United States v. Starr*, the proper inquiry regarding the legal meaning of a statute is as follows:

> It is the function of the legislature to make the laws and the duty of judges to interpret them. 2A Norman J. Singer, *Sutherland Statutory Construction* § 45.03 (4th ed. 1984). Judges should interpret a statute so as to carry out the will of the legislature. *United States v. Dickenson*, 20 C.M.R. 154, 165 (C.M.A. 1955). Otherwise, they violate the principle of the separation of powers. Singer, *supra*, § 45.05. "If the words used in the statute convey a clear and definite meaning, a court has no right to look for or to impose a different meaning." *Dickenson*, 20 C.M.R. at 165. Thus, in interpreting a statute, we employ the following process: (1) Give the operative terms of the statute their ordinary meaning; if the terms are unambiguous, the inquiry is over; (2) If the operative terms of the statute are

[2] If the Government claims, as it did with the Motion to Dismiss the Article 104 Offense, that the charges should not be dismissed because the specification is sufficient, the Defense would like to clarify that its argument is not that the specification is deficient; it is that the theory underlying the specification is deficient. This is appropriately styled as a motion to dismiss for failure to state an offense. *See, e.g., United States v. Nosal* (*Nosal III*), ___ F.3d ___, No. 10-10038, 2012 WL 1176119, at *8 (9th Cir. April 10, 2012) (en banc) (holding that the district court's dismissal of the counts of the indictment alleging violations of Section 1030 was proper because the Government's theory of "exceeds authorized access" was erroneous).

[3] The term "exceeds authorized access" or some derivative thereof appears in several provisions of Section 1030. *See, e.g.*, 18 U.S.C. § 1030(a)(1) ("exceeding authorized access"); *id.* § 1030(a)(2) ("exceeds authorized access"); *id.* § 1030(a)(4) (same); *id.* § 1030(a)(7)(B) ("in excess of authorization" and "exceeding authorized access"). These phrases are nearly identical and "identical words and phrases within the same statute should normally be given the same meaning." *Nosal III*, 2012 WL 1176119, at *4 (quoting *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007)) (internal quotations omitted). Thus, the interpretation of the term "exceeds authorized access" contained in Section 1030(e)(6) applies to all variants of the term used, including "exceeding authorized access" in Section 1030(a)(1). *See id.* ("Congress obviously meant 'exceeds authorized access' to have the same meaning throughout [S]ection 1030.").

> ambiguous, then we examine the purpose of the statute as well as its legislative history; and (3) If a reasonable ambiguity still exists, then we apply the rule of lenity and resolve the ambiguity in favor of the accused. *See United States v. Ferguson*, 40 M.J. 823, 830 (N.M.C.M.R. 1994).

51 M.J. 528, 532 (A.F. Ct. Crim. App. 1999); *see also United States v. McGuinness*, 33 M.J. 781, 784-85 (N.M.C.M.R. 1991) ("First, a court should give all the terms used in the statute their ordinary meaning. Second, if a possible ambiguity exists in the statute when a term's ordinary meaning is used, then a court must examine the legislative history and motivating policies of Congress in enacting the statute to resolve the ambiguity. And finally, if after applying steps one and two, a reasonable doubt still exists about a statute's intended scope, then the Court will apply the rule of lenity and resolve the ambiguity in favor of the appellant.").

12. The term "exceeds authorized access" in Section 1030 has a clear legal meaning. A person exceeds authorized access under Section 1030(a)(1) when, despite being authorized to use the computer, the accused uses his access to the computer to obtain or alter information in the computer that he is not entitled to obtain or alter. Section 1030 is thus concerned only with bypassing technical restrictions on access, not the improper purpose for which one has accessed the information. Alternatively, if this Court determines that the statutory language is ambiguous (which the Defense believes it is not), then the purpose of the statute and the legislative history clearly indicate that Section 1030 was not intended to address misuse of information, only misuse of the computer, in the sense of hacking or bypassing technical restrictions. If, after a review of the plain language and legislative history, the Court concludes that there is still ambiguity, then that ambiguity must be resolved in favor of the accused under the rule of lenity.

13. Section 1030(a)(1) punishes:

> Whoever --
>
> (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government . . . to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it[.]

18 U.S.C. § 1030(a)(1). In this case, the Government has proceeded under the theory that PFC Manning knowingly exceeded his authorized access in accessing certain information and disclosing that information to persons not authorized to receive it, in contravention of the Government's Acceptable Use Policy and/or that PFC Manning accessed information for an improper purpose. Notably, the Government has not alleged that PFC Manning accessed a

computer that he was not entitled to access. Nor has the Government alleged that PFC Manning accessed information on the computer that he was not entitled to access.

14. Congress has provided a definition for "exceeds authorized access" in Section 1030(e)(6): "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]" *Id.* § 1030(e)(6).[4] This language is plain and unambiguous. *See United States v. Inthavong*, 48 M.J. 628, 630 (A. Ct. Crim. App. 1998) ("[S]tatutory ambiguity may not be manufactured as a device to defeat manifest congressional intent."). An accused exceeds authorized access under Section 1030(a)(1) when, despite being authorized to use the *computer*, the accused uses his access to the computer to obtain or alter *information* in the computer that he is not entitled to obtain or alter.

15. For instance, if PFC Manning had used his government computer (to which he has authorized access) to hack into the White House server and obtain President Obama's official e-mails, he would presumably be "exceeding authorized access." Likewise, if PFC Manning had used his government computer (to which he has authorized access) to change the contents of diplomatic cables on the server, he would be "exceeding authorized access." In short, the section is intended to punish those who, while authorized to use the computer, bypass technical restrictions and use the computer to access or alter information that they are not allowed to access or alter. The section does not extend to the situation where the user has authorization to access the information in question, but somehow misuses or misappropriates that information. *See United States v. Nosal* (*Nosal III*), ___ F.3d ___, No. 10-10038, 2012 WL 1176119, at *7-8 (9th Cir. April 10, 2012) (en banc); *United States v. Aleynikov*, 737 F. Supp. 2d 173, 192 (S.D.N.Y. 2010); *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ("The plain language of [Section 1030] supports a narrow reading. [Section 1030] expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation."); *see also Xcedex, Inc. v. VMware, Inc.*, No. 10-3589 (PJS/JJK), 2011 WL 2600688, at *4 (D. Minn. June 8, 2011) ("[Section 1030] itself defines 'exceeds authorized access' as 'access[ing] a computer with authorization and [using] 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). Therefore, 'without authorization' and 'exceed[ing] authorized access' depend on the 'unauthorized use of *access*,' not on the 'unauthorized use of *information*.'" (emphasis in original)); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) ("[T]he plain language of [Section] 1030(a)(2), (4), and (5)(A)(iii) target 'the unauthorized procurement or alteration of information, not its misuse or misappropriation.'").

16. PFC Manning clearly had authorization to access the government computers in question.

[4] Section 1030(a)(1) today uses the phrase "exceeding authorized access" instead of "exceeds authorized access." 18 U.S.C. § 1030(a)(1). This subsection was amended in 1996 by substituting the term "exceeding" for the term "exceeds," which had been used in that subsection since 1986. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201(1)(A)(ii), 110 Stat. 3488, 3491. The change in phrasing was likely grammatical only and the definition of "exceeds authorized access" in Section 1030(e)(6) is likely still applicable to the term "exceeding authorized access" in Section 1030(a)(1). *See* S. Rep.104-357 (1996) ("The amendment specifically covers the conduct of a person who deliberately breaks into a computer without authority, or an insider who *exceeds authorized access*, and thereby obtains classified information and then communicates the information to another person, or retains it without delivering it to the proper authorities." (emphasis supplied)).

Thus, the only remaining question is whether the Government alleges that PFC Manning "exceed[ed] authorized access" within the meaning of Section 1030 – i.e. whether he "obtain[ed] or alter[ed] information in the computer that [he was] not entitled so to obtain or alter[.]" 18 U.S.C. § 1030(e)(6). The Government has not alleged that PFC Manning used his access to obtain information that he was not entitled to obtain. On the contrary, the Government will concede that PFC Manning was authorized to obtain each and every piece of information that he allegedly accessed. Similarly, the Government has not alleged that PFC Manning altered any of the information that he allegedly accessed. Instead, the Government alleges that because PFC Manning had an improper purpose in accessing the information that he had full permission to access, he has exceeded authorized access within the meaning of the statute. This is an incorrect reading of the term "exceeds authorized access" – and one which conflicts with the plain meaning of the statute. *See Walsh Bishop Assocs., Inc. v. O'Brien*, No. 11-2673 (DSD/AJB), 2012 WL 669069, at *3 (D. Minn. Feb. 28, 2012) ("The language of [Section] 1030(a)(2) does not support the interpretation of Walsh Bishop. Instead, Walsh Bishop's interpretation requires the court to rewrite the statute to replace the phrase 'to use such access to obtain or alter information that the accesser is not entitled so to obtain or alter' with 'to use such information in a manner that the accesser is not entitled so to use.' But subsection (a)(2) is not based on use of information; it concerns access. Indeed, the language of subsection (a)(1) shows that Congress knows how to target the use of information when it intends to do so."); *United States v. Zhang*, No. CR-05-00812 RMW, 2010 WL 4807098, at *3 (N.D. Cal. Nov. 19, 2010) ("Nonetheless, a plain reading of [S]ection 1030(e)(6)'s definition . . . compels a different conclusion. An individual 'exceeds authorized access' if he or she has permission to access a portion of the computer system but uses that access to 'obtain or alter information in the computer that [he or she] is not entitled so to obtain or alter.' As the court in *Norsal* [sic] explained, 'there is simply no way to read that definition to incorporate policies governing use of information unless the word alter is interpreted to mean misappropriate.'" (citations omitted)).

17. The plain language of "exceeds authorized access" is further supported by looking at the specification itself. The Government alleges:

> In that Private First Class Bradley E. Manning, U.S. Army, did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, having knowingly *exceeded authorized access* on a Secret Internet Protocol Router Network computer, *and by means of such conduct having obtained 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, to wit: more than seventy-five classified United States Department of State cables[.]

Charge Sheet, Specification 13 (emphasis supplied). It is clear that "exceeding authorized access" is different from, and a predicate to, "obtaining information." If the term "exceeded authorized access" is interpreted as the Government suggests, the charge would be redundant and nonsensical:

> In that Private First Class Bradley E. Manning, U.S. Army, did, at or near

> Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, having knowingly ["accessed that computer … to obtain these documents," *see* Oral Argument, Unauthenticated Transcript, *supra*] on a Secret Internet Protocol Router Network computer, and by means of such conduct having obtained 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, to wit: more than seventy-five classified United States Department of State cables[.]

Charge Sheet, Specification 13 (alteration supplied). Thus read, the charge does not make sense since "exceeding authorized access" is conflated with obtaining documents for an improper purpose, which is the next part of the charge ("by means of such conduct having obtained information"). Thus, the exceeding authorized access cannot be the same as "obtain[ing] information" or the specification falls apart. This provides further evidence that the plain meaning of the statute is clear: Section 1030 asks only whether the accused had authorized access to the computer and information in question. It does not contemplate an inquiry into what an accused otherwise does with properly accessed information.

B. The Legislative History of 18 U.S.C. Section 1030 Clearly Shows that "Exceeding Authorized Access" Does Not Involve an Inquiry into the Purposes for Which the Information is Used

18. The legislative history of Section 1030 leaves no doubt that "exceeding authorized access" is strictly limited to the question of whether the accused who had authorized access to the computer, accessed information that he was not entitled to access. It does not encompass an analysis into the purposes for which information accessed with authorization is ultimately used. Otherwise stated, the section is intended to criminalize intruders who trespass on computer networks, in the sense of circumventing technological restrictions on access. It is not intended to criminalize the acts of those persons who, while authorized to access the information in question, happen to use computers in carrying out an underlying criminal offense.[5] In 2008, the Congressional Research Service issued a report which analyzed Section 1030 and specifically acknowledged that the statute "outlaws conduct that victimizes computers. It is a computer security law. It protects computers in which there is a federal interest." Charles Doyle, Cong. Research Service, *Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws* 1 (2008). Just as most modern jurisdictions have trespass laws, intended to protect real property – as opposed to larceny laws protecting the chattel located on that property – Section 1030 was passed to protect computers, not the information located on those computers.

19. Section 1030 was originally enacted in 1984. Act of Oct. 12, 1984, Pub. L. No. 98-473, §§ 2101-2103, 98 Stat. 1837, 2190-92. In that 1984 version, Section 1030(a)(1) punished whoever

[5] Indeed, this would seem to be a common sense proposition. An act which is carried out through the use of a computer is not more culpable or criminal than one which is carried out without the use of a computer. That is, the alleged disclosure of documents to WikiLeaks through a computer should not carry a greater penalty than the alleged disclosure of paper documents to the same organization. The use of the computer in carrying out the alleged offense should not result in greater legal punishment.

> knowingly accesses a computer without authorization, *or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend*, and by means of such conduct obtains information that has been determined by the United States Government . . . to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.

Id. § 2102(a), 98 Stat. 2190 (emphasis supplied). In 1986, Congress replaced the phrase "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" with the phrase "or exceeds authorized access." Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(c), 100 Stat. 1213. In the same Act, Congress added to Section 1030 the definition of "exceeds authorized access" that is presently codified at Section 1030(e)(6). *Id.* § 2(g)(4); *see* 18 U.S.C. § 1030(e)(6).

20. This significant change in language in Section 1030(a)(1) belies any argument that the term "exceeds authorized access" extends to situations where an accused who has authorization to use the computer uses the access for *purposes* to which the authorization does not extend. Clearly, Congress was quite capable of drafting language which would criminalize using a computer or the information contained therein in a way that is inconsistent with the governing terms of use or the computer owner's interests. The language in the prior statute covered this situation perfectly; it criminalized the scenario where a person "uses the opportunity that such [authorized] access provides for purposes to which such authorization does not extend." Pub. L. No. 98-473, § 2102, 98 Stat. at 2190; *see Walsh Bishop Assocs., Inc.*, 2012 WL 669069, at *3 ("Further, the legislative purpose and history supports the plain meaning of the statute. Congress enacted [Section 1030] to deter 'the criminal element from abusing computer technology in future frauds.' H.R. Rep. No. 98–894, at 4 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3690. As originally enacted, [Section 1030] applied to a person who (1) knowingly accessed without authorization or (2) 'having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.' Pub. L. No. 98–473, § 2102, 98 Stat. 2190, 2190–91 (1984). Congress amended the statute by replacing the latter means of access with the phrase 'exceeds authorized access.' *See* Pub. L. No. 99–474, § 2, 100 Stat. 1213, 1213 (1986). The stated reason for the amendment was to 'eliminate coverage for authorized access that aims at purposes to which such authorization does not extend.' *See* S. Rep. No. 99–432, at 21 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2495 (internal quotation marks omitted). As a result, Congress amended the statute to remove use as a basis for exceeding authorization."); *Condux Int'l, Inc. v. Haugum*, No. 08-4824 ADM/JSM, 2008 WL 5244818, at *5 (D. Minn. Dec. 15, 2008) ("Had Congress [under Section 1030] intended to target how a person makes use of information, it would have explicitly provided language to that effect.").

21. In the Senate report on the 1986 amendment of this phrase, Senators Mathias and Leahy commented favorably on the substitution of "exceeds authorized access" for the pre-1986 language of Section 1030:

> [The 1986 Amendments] would eliminate coverage for unauthorized access that aims at "purposes to which such authorization does not extend." This removes from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization.

S. Rep. No. 99-432, at 21, *reprinted in* 1986 U.S.C.C.A.N. at 2494-95; [6] *see also Aleynikov*, 737 F. Supp. 2d at 192-93 n.23 (discussing legislative history behind 1986 amendments to the language of Section 1030); *Shamrock Foods*, 535 F. Supp. 2d at 966 ("[T]he legislative history confirms that [Section 1030] was intended to prohibit electronic trespassing, not the subsequent use or misuse of information."); *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005) (explaining the purpose of the change in legislative language).

22. Additionally, when Congress amended Section 1030(a)(1) in 1996, it helpfully clarified the interplay between that section and the espionage statutes:

> Although there is considerable overlap between 18 U.S.C. [Section] 793(e) and [S]ection 1030(a)(1), as amended by the NII Protection Act, the two statutes would not reach exactly the same conduct. Section 1030(a)(1) would target those persons who deliberately *break into a computer* to obtain properly classified Government secrets then try to peddle those secrets to others, including foreign governments. In other words, unlike existing espionage laws prohibiting the theft and peddling of Government secrets to foreign agents, [S]ection 1030(a)(1) would require proof that the individual knowingly used a computer without authority, or in excess of authority, for the purpose of obtaining classified information. In this sense then, *it is the use of the computer which is being proscribed*, not the unauthorized possession of, access to, or control over the classified information itself.

S. Rep. No. 104-357 (1996) (emphases supplied). As this passage makes clear, a person's intent in accessing the computer (e.g., to steal government secrets) is entirely distinct from the inquiry of whether that person has authorization to access the computer or information in question (i.e. whether that person is in essence "breaking into" that computer). A purpose to steal government information may be relevant to a prosecution under 18 U.S.C. Section 793(e), which prohibits theft and peddling of government secrets. However, that purpose cannot determine whether a person has "broken into" a computer by accessing it without authority or by accessing information in excess of his authority.

[6] By way of elaboration, Congress never actually intended to give the Computer Crimes Fraud Act such expansive interpretation. Senators Mathias and Leahy appended their own statement to the Report and explained in more detail the reason for the 1986 amendments. They explained how the original version of the CFAA had been passed in haste, as part of a legislative rider. *See* S. Rep. No. 99-432, at 20-21, *reprinted in* 1986 U.S.C.C.A.N. at 2494. As a result, in 1984, the House had never voted on a series of narrowing amendments, which had been unanimously approved by the Senate. The purpose of the 1986 amendments was to fix the shortcomings of the original version. *See id*. at 20-22.

23. That Congress intended for Section 1030 to criminalize computer crimes, and not the underlying criminal or tortious conduct carried out on the computer, is readily apparent from looking at the full name of the statute – the Computer Fraud and Abuse Act (CFAA). The primary purpose of the CFAA "was to create a cause of action against computer hackers (e.g., electronic trespassers)." *Int'l Ass'n of Machinists & Aerospace Workers,* 390 F. Supp. 2d at 495 (quoting *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000)) (internal quotations omitted). As the House Report explained, the bill was aimed largely at hackers who "trespass into" computers: "[T]he conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer . . . in committing the offense." H.R. Rep. No. 98-894, at 20 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706. As Professor Orin Kerr argues:

> [T]he available evidence suggests that legislators mostly saw such statutes as doing for computers what trespass and burglary laws did for real property. For example, the House Report on the first federal computer crime legislation passed in 1984 noted that "[S]ection 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense." Several state statutes incorporated this concept into the titles of their computer crime statutes, labeling the new unauthorized access crimes as crimes of "Computer Trespass." The legislative histories of computer crime laws also regularly refer to the activity prohibited by unauthorized access statutes as computer trespasses or "breaking into computer systems."

Orrin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1617-18 (2003) [hereinafter Kerr, *Cybercrime's Scope*] (footnotes omitted).

24. Thus, the legislative history of both: a) the term "exceeds authorized access" and; b) the CFAA as a whole, clearly reveal what Congress intended when it enacted the statute. It intended that the section would criminalize those who strayed beyond the technical authorization they were given. It did not intend to criminalize those who used a computer for an improper purpose or in contravention of the governing terms of use, even if that use amounted to a criminal offense.

C. Case Law Supports the View that An Accused's Purpose in Accessing the Computer or the Information is Entirely Irrelevant to Whether an Accused "Exceeded Authorized Access" Under 18 U.S.C. Section 1030(a)(1)

25. A large number of courts have appropriately applied the plain meaning of Section 1030 and thus distinguished between two very distinct scenarios: exceeding authorized *access* and exceeding authorized *use*. *See Nosal III*, 2012 WL 1176119, at *8; *Aleynikov*, 737 F. Supp. 2d at 192; *Zhang*, 2010 WL 4807098, at *3. This interpretation of "exceeds authorized access" has been adopted in the civil context as well. *See, e.g., Walsh Bishop Assocs., Inc.*, 2012 WL

669069, at *2-3; *Xcedex, Inc.*, 2011 WL 2600688, at *4; *Océ N. Am., Inc. v. MCS Servs., Inc.*, 748 F. Supp. 2d 481, 485-87 (D. Md. 2010); *AtPAC, Inc. v. Aptitude Solutions, Inc.*, 730 F. Supp. 2d 1174, 1181 (E.D. Cal. 2010); *Univ. Sports Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 283-85 (S.D.N.Y. 2010); *Lewis-Burke Assocs. LLC v. Widder*, 725 F. Supp. 2d 187, 192-94 (D.D.C. 2010); *Orbit One Commc'ns, Inc.*, 692 F. Supp. 2d at 385-86; *Bell Aerospace Servs., Inc. v. United States Aero Servs., Inc.*, 690 F. Supp. 2d 1267, 1272 (M.D. Ala. 2010) ("'Exceeds authorized access' should not be confused with exceeds authorized use."); *ReMedPar, Inc. v. Allparts Med., LLC*, 683 F. Supp. 2d 605, 610-13 (M.D. Tenn. 2010); *Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp. 2d 378, 406-07 (E.D. Pa. 2009); *Jet One Group, Inc. v. Halcyon Jet Holdings, Inc.*, No. 08-CV-3980 (JS)(ETB), 2009 WL 2524864, at *5-6 (E.D.N.Y. Aug. 14, 2009); *State Analysis, Inc. v. Am. Fin.. Servs. Assoc.*, 621 F. Supp. 2d 309, 315-17 (E.D. Va. 2009); *Condux Int'l, Inc.*, 2008 WL 5244818, at *4-6; *Int'l Ass'n of Machinists & Aerospace Workers*, 390 F. Supp. 2d at 498-99.

26. This proper interpretation was most recently adopted by the en banc Ninth Circuit Court of Appeals in *Nosal III*. In *Nosal III*, employees of the defendant's former employer, using their accounts to access the employer's computer system, provided the defendant with trade secrets and other proprietary information of the employer. 2012 WL 1176119, at *1. The employer placed several limitations on its employees' access of its system, including a restriction on the use or disclosure of all information available on that system, except for legitimate company business. *Id.* at *1 & n.1. The defendant was charged with aiding and abetting the employees' violations of Section 1030(a)(4).[7] *Id.* at *1. The defendant moved to dismiss the counts of the indictment alleging violations of Section 1030(a)(4), "arguing that the statute targets only hackers, not individuals who access a computer with authorization but then misuse information they obtain by means of such access." *Id.* The district court ultimately agreed with the defendant's position and granted the motion to dismiss. *Id.*

27. A majority of a panel of three judges of the Ninth Circuit reversed, holding that "an employee 'exceeds authorized access' under [Section] 1030 when he or she violates the employer's access restrictions – including use restrictions." *United States v. Nosal* (*Nosal I*), 642 F.3d 781, 785 (9th Cir. 2011), *reh'g en banc granted*, 661 F.3d 1180 (9th Cir. 2011). To support its expansive interpretation, the majority focused on one word in the definition of "exceeds authorized access" provided in Section 1030(e)(6): "so." *See Nosal I*, 642 F.3d at 785-86. The court reasoned that the word "'[s]o' in this context means 'in a manner or way that is indicated or suggested.'" *Id.* at 785 (quoting *Webster's Third New Int'l Dictionary* 2159 (Philip Babcock Gove, ed. 2002)). In her dissent, Judge Campbell identified two major flaws with the panel opinion: its reliance on the word "so" was misplaced, and its interpretation of the term "exceeds authorized access" rendered at least one provision of Section 1030 unconstitutionally vague. *Id.* at 789-91 (Campbell, J., dissenting).

---

[7] Section 1030(a)(4) punishes whoever

> knowingly and with intent to defraud, accesses a protected computer without authorization, *or exceeds authorized access*, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period[.]

18 U.S.C. § 1030(a)(4) (emphasis supplied).

28. After granting the defendant's petition for rehearing en banc and withdrawing the panel opinion, *see United States v Nosal* (*Nosal II*), 661 F.3d 1180, 1180 (9th Cir. 2011), the en banc Ninth Circuit, in a 9-2 opinion authored by Chief Judge Kozinski, affirmed the district court's dismissal of the Section 1030 counts of the defendant's indictment. *See Nosal III*, 2012 WL 1176119, at *8. The court held that "'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*." *Id.* (emphases in original). The *Nosal III* Court found this interpretation of "exceeds authorized access" to be most consistent with the statutory text and structure of the CFAA, as well as the legislative history of that statute.

29. The court first explained why the word "so" in Section 1030(e)(6)'s definition of "exceeds authorized access" could not bear the weight the Government and the panel majority assigned to it:

> The government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. This places a great deal of weight on a two-letter word that is essentially a conjunction. If 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. at *2. Moreover, "Congress could just as well have included 'so' as a connector or for emphasis." *Id.*

30. The *Nosal III* Court also reasoned that interpreting the phrase "exceeds authorized access" to only proscribe violations of access restrictions, and not violations of use restrictions, would be most consistent with the structure of the CFAA as a whole. *Id.* at *3-4. Because the phrase is used in several different provisions of the CFAA, the court was mindful that its interpretation of the phrase would control each provision of Section 1030 in which the phrase appears. *See id.* at *4. The court was troubled with the effect the Government's interpretation would have on one particular provision of the CFAA:

> Subsection 1030(a)(2)(C) requires only that the person who "exceeds authorized access" have "obtain[ed] . . . information from any protected computer." Because "protected computer" is defined as a computer affected by or involved in interstate commerce – effectively all computers with Internet access – the government's interpretation of "exceeds authorized access" makes every violation of a private computer use policy a federal crime.

Id. at *3 (ellipsis and alteration in original). This scenario would pose serious notice and arbitrary enforcement concerns. *See id.* at *3-6 (discussing these concerns); *see also* Part E, *infra* (explaining the *Nosal III* Court's discussion of these concerns).

31. Finally, the *Nosal III* Court determined that its interpretation was most consistent with the CFAA's overarching purpose and legislative history. *Nosal III*, 2012 WL 1176119, at *3. Congress's primary aim in enacting the CFAA was to target computer hacking. *Id.* The court explained how its interpretation of the term "exceeds authorized access" kept this purpose in mind:

> [I]t is possible to read both prohibitions as applying to hackers: "[W]ithout authorization" would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and "exceeds authorized access" would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files). This is a perfectly plausible construction of the statutory language that maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate.

Id. (emphases in original). The court went on to note that Congress's replacement of the phrase "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" with the phrase "exceeds authorized access" further supported its interpretation of that term, and further undermined the Government's proposed interpretation. *Id.* at *3 n.5.

32. The United States District Court for the Southern District of New York reached the same conclusion in *United States v. Aleynikov*. In *Aleynikov*, the defendant, a Goldman Sachs computer programmer copied, compressed, encrypted and transferred hundreds of thousands of lines of Goldman Sachs' source code, which he later gave to his new employer. 737 F. Supp. 2d at 174-75. The defendant was authorized to access the Goldman computer he accessed and to access the source code he accessed, though Goldman Sachs required each computer programmer to sign a confidentiality agreement and limited access to its source code to those employees who have reason to access it. *Id.* at 175, 190-91. The defendant was indicted for unauthorized access and exceeding authorized access under Section 1030(a)(2)(C). *Id.* at 190. The defendant moved to dismiss this count of the indictment, arguing that Section 1030 "does not encompass an employee's misuse or misappropriation of information that the employee has authority to access." *Id.* at 191.

33. The court granted the defendant's motion to dismiss the Section 1030(a)(2)(C) count of the indictment and held that "a person who 'exceeds authorized access' has permission to access the computer, but not the particular information on the computer that is at issue." *Id.* at 191-92. The court explained that:

> Section 1030(a)(2)(C) therefore addresses only the unauthorized procurement or alteration of information. The phrase[ ] . . ."exceeds authorized access" *cannot be read to encompass an individual's misuse or misappropriation of information to which the individual was permitted access. What use an individual makes of the accessed information is utterly distinct from whether the access was authorized in the first place*. The Government's theory that [Section 1030] is violated whenever an individual uses information on a computer in a manner contrary to

> the information owner's interest would therefore require a departure from the plain meaning of the statutory text.

Id. at 192 (emphasis supplied). The court further explained that its interpretation was consistent with the statutory text, the overall purpose and structure of Section 1030, and the legislative history of the section. *Id.* at 192-93 & n.23.

34. The Ninth Circuit also reached a similar result in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (2009).[8] In that case, an employer brought an action against its former employee under Section 1030(g),[9] alleging that the former employee exceeded authorized access when he emailed documents to himself and his wife "to further his own personal interests, rather than the interests of [his employer]." *Brekka*, 581 F.3d at 1132; *see id.* at 1129-30. The Court rejected the plaintiff's reading of the phrase "exceeds authorized access:"

> No language in the CFAA supports LVRC's argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest. Rather, the definition of "exceeds authorized access" in [Section] 1030(e)(6) indicates that Congress did not intend to include such an implicit limitation in the word "authorization." Section 1030(e)(6) provides: "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) . . . . In other words, for purposes of the CFAA, 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. It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or "without authorization."
>
> This leads to a sensible interpretation of [Sections] 1030(a)(2) and (4), which gives effect to both the phrase "without authorization" and the phrase "exceeds authorized access": a person who "intentionally accesses a computer without authorization," §§ 1030(a)(2) and (4), accesses a computer without any permission at all, while a person who "exceeds authorized access," *id.*, has permission to access the computer, but accesses information on the computer that the person is not entitled to access.

Id. at 1133. This reasoning was also echoed by the court in *International Association of Machinists & Aerospace Workers*, where 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

[8] Although *Brekka* is a civil case, it involves the interpretation of a criminal statute. As the *Brekka* court itself notes, its interpretation "is equally applicable in the criminal context." 581 F.3d at 1134. With that said, civil cases that use an expansive interpretation of Section 1030 should be viewed with extreme caution. *See* note 10, *infra*.
[9] 18 U.S.C. Section 1030(g) provides a right of action for private persons injured by computer crimes.

business. 390 F. Supp. 2d 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.* at 498. The court rejected the application of Section 1030, holding that even if the defendant breached a contract, 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 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 498-99 (emphasis in original). The court captured the issue perfectly when it explained that "the gravamen of [the] complaint is not so much that [the accused] improperly accessed the information . . . but rather what [the accused] did with the information once [the accused] obtained it." *Id.* at 499. The Government in the instant case has made the same mistake. The gravamen of the offense alleged is that PFC Manning allegedly transmitted classified information to persons not authorized to receive it. It just so happens that a computer was the means by which he is alleged to have done so. This does not, in any circumstances, mean that PFC Manning exceeded authorized access within the meaning of Section 1030.

35. These cases are representative of the host of other cases that have properly interpreted the term "exceeds authorized access" in Section 1030. *See, e.g., Walsh Bishop Assocs., Inc.*, 2012 WL 669069, at *2-3; *Xcedex, Inc.*, 2011 WL 2600688, at *4; *Océ N. Am., Inc.*, 748 F. Supp. 2d at 485-87 (identifying that the phrase "exceeds authorized access" exclusively prohibits access of a computer without authorization, not an employee's misuse of information that the individual was permitted to access); *AtPac, Inc.*, 730 F. Supp. 2d at 1181 ("[T]he definition of the term 'exceeds authorized access' is one that simply examines whether the accessor was entitled to access the information for any purpose."); *Univ. Sports Publ'ns Co.*, 725 F. Supp. 2d at 283-85; *Lewis-Burke Assocs. LLC*, 725 F. Supp. 2d at 194 (explaining that "'[e]xceeds authorized access' should not be confused with exceeds authorized use." (internal quotations omitted)); *Orbit One Commc'ns, Inc.*, 692 F. Supp. 2d at 385-86; *Bell Aerospace Servs, Inc.*, 690 F. Supp. 2d at 1272 ("'Exceeds authorized access' should not be confused with exceeds authorized use."); *ReMedPar, Inc.*, 683 F. Supp. 2d at 610-13 (recognizing that "exceeds authorized use" is to be construed narrowly, reasoning that the phrase is not intended to extend to situations where the access was authorized but the use was not); *Bro-Tech Corp.*, 651 F. Supp. 2d at 407 (A defendant's purpose in accessing a computer is irrelevant to whether he or she exceeds authorized access, even if the purpose in doing so is to misuse or misappropriate the information); *Jet One Group, Inc.*, 2009 WL 2524864, at *5-6; *State Analysis, Inc.*, 621 F. Supp. 2d at 317 (recognizing that "exceeds authorization" is explicitly 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." (internal quotations omitted)); *Condux Int'l, Inc.*, 2008 WL 5244818, at *4-6; *Shamrock Foods*, 535 F. Supp. 2d 962 (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); *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (identifying the narrower interpretation of "exceeding authorized access" as "the more reasoned view," and holding 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."); *Int'l Ass'n of Machinists & Aerospace Workers*, 390 F. Supp. 2d at 498-99.

36. Notwithstanding Congress's clear and unambiguous definition of "exceeds authorized access" in Section 1030(e)(6), some courts have erroneously held that the purpose for which a computer or information is accessed is somehow relevant to the inquiry of whether the accused exceeded his authorized access.[10] *See, e.g., United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010) ("[T]he concept of 'exceeds authorized access' may include exceeding the purposes for which the access is 'authorized.' Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."). These cases are wrongly decided. Neither the *John* Court nor the *Rodriguez* Court offered any explanation – much less any plausible explanation – as to how its interpretation of "exceeds authorized access" could be squared with the plain meaning of Section 1030. As the court stated in *Aleynikov*:

[10] Many of the cases that hold that a user's purpose in accessing the computer is relevant to a charge under Section 1030 have been decided in the civil context. These civil cases are inapposite and their reasoning should not be extrapolated to the criminal context. In civil cases, the defendant risks having to pay a fine under Section 1030; in criminal cases, the defendant faces the potential for physical confinement. It stands to reason that civil courts will interpret Section 1030 more broadly than criminal courts. This point is clearly made by Professor Kerr:

> The second source of the difficulty is that many cases have interpreted "authorization" in the context of civil disputes rather than criminal prosecutions. The difference tends to push courts in the direction of expansive interpretations of new laws. It is one thing to say that a defendant must pay a plaintiff for the harm his action caused; it is quite another to say that a defendant must go to jail for it. Courts are more likely to hold a defendant liable under an ambiguous statute when the stakes involve a business dispute between two competitors than when the government seeks to punish an individual with jail time. As a result, civil precedents tend to adopt broader standards of liability than do criminal precedents. Because many unauthorized access cases have arisen in a civil context with sympathetic facts, courts have adopted broad approaches to authorization that in a criminal context would criminalize a remarkable swath of conduct involving computers.

Kerr, *Cybercrime's Scope*, *supra*, at 1641-42.

> [These cases] identify no statutory language that supports interpreting [Section 1030] to reach misuse or misappropriation of information that is lawfully accessed. Instead, they improperly infer that "authorization" is automatically terminated where an individual "exceed[s] *the purposes* for which access is 'authorized.'" But "the definition of 'exceeds authorized access' in [Section] 1030(e)(6) indicates that Congress did not intend to include such an implicit limitation in the word 'authorization.'"

737 F. Supp. 2d at 193 (emphasis supplied) (citations omitted).

37. The en banc *Nosal* Court further pointed out that the *Rodriguez* and *John* decisions were the product of the courts' failure to consider the broader implications of their holdings. The *Nosal III* Court explained that:

> These courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of "exceeds authorized access." They therefore failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to avoid "making criminal law in Congress's stead."

2012 WL 1176119, at *6 (quoting *United States v. Santos*, 553 U.S. 507, 514 (2008) (plurality opinion)).

38. Finally, neither the defendant in *John* nor the defendant in *Rodriguez* brought to the court's attention the very significant 1986 amendment to Section 1030's text replacing the phrase "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend" with the phrase "exceeds authorized access." *See* Brief for Defendant-Appellant, *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (No. 09-15265), 2010 WL 5650308; Reply Brief for Defendant-Appellant, *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (No. 09-15265), 2010 WL 5650310; Brief for Defendant-Appellant, *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (No. 08-10459), 2008 WL 7986381; Reply Brief for Defendant-Appellant, *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (No. 08-10459), 2008 WL 7986383. The Government in each case similarly failed to discuss this crucial piece of legislative history. *See* Brief for Appellee United States, *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (No. 09-15265), 2010 WL 5650309; Brief for Appellee United States, *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (No. 08-10459), 2008 WL 7986382. Had they done so, the result would likely have been different.

39. The imprudent expansive interpretation of "exceeds authorized access" adopted by the *Rodriguez* and *John* courts should be rejected because it is inconsistent with the plain text of Section 1030 and contrary to congressional intent.

40. As discussed, the plain language of Section 1030(e)(6) in no way indicates that the purposes of an accused in accessing the information or violations of access restrictions can establish that an accused has exceeded authorized access if he has authority to access the computer and to access the information. *See* 18 U.S.C. § 1030(e)(6) ("[T]he term 'exceeds authorized access'

means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]"). If the accused has authorization to access the computer and obtains information that the accused has authorization to obtain, the accused cannot, under the plain language of Section 1030(e)(6), be held to have exceeded his authorized access. Interpreting "exceeds authorized access" to include an accused's misuse of information or violation of access restrictions is inconsistent with the plain language of Section 1030(e)(6) and with the legislative history of Section 1030.

41. Even if a court could "get past" the problems with statutory interpretation, there is another serious infirmity in the interpretation advanced by courts that ascribe an expansive interpretation of Section 1030. These courts require an analysis into an accused's subjective intent at the time he accessed the relevant information in order to determine whether he exceeded his authorized access. In other words, "exceeding authorized access" becomes a shifting standard depending on a person's intent at the time they accessed the information. For instance, consider a corporate lawyer who uses his employer's computer to search for information on what deals the firm is working on. He has full access to the firm's computers and full authority to access and read client files. As he is perusing the files, he discovers information that a corporate client has overstated its revenues and would be issuing a public statement to that effect the subsequent week. He owns shares of that company and, based on the information he has acquired, decides a few days later to sell his shares. The law firm's terms of use specify that lawyers may not use firm information for their personal financial gain. Has the lawyer "exceeded authorized access" because he violated the terms of use? Certainly, the lawyer may be guilty of insider trading or may have violated ethical canons – but he did not exceed authorized access under the expansive (and incorrect) interpretation of Section 1030 because, at the time he accessed the information, he had no intent to use the information for a purpose contrary to the terms of use. If, however, the lawyer went looking for information on the computer on the particular client with the intention of using it for his own purposes, under the interpretation offered by *Rodriguez* and *John*, the lawyer would be exceeding authorized access because he exceeded the firm's terms of use. Thus, the very same act – looking at the financial information of a corporate client – would be punishable under Section 1030 in some cases, but not in others.[11]

42. This variable standard cannot be what Congress intended. Either a person has exceeded authorized access (in that they accessed information that they did not have permission to access) or they did not. The determination cannot be a nebulous inquiry into an accused's state of mind at the time he accessed material that he had authorization to access. *See Aleynikov*, 737 F. Supp. 2d at 194 ("The interpretation of [Section 1030] adopted in this line of cases would require an analysis of an individual's subjective intent in accessing a computer system, whereas the text of

[11] Indeed, the en banc Ninth Circuit raised this very possibility in the *Nosal* rehearing in reference to a hypothetical defendant who sold security information to a hostile power. One judge asked, "Does the employee violate the Act if the employee has security clearance to be into the database but the government has said, 'You may access this database as long as you don't sell it to a hostile power.' And somebody takes the information to which they are authorized to be there by virtue of their security clearance but then takes it and sells it to a hostile power?" Oral Argument at 14:14, *United States v. Nosal*, No. 10-10038 (9th Cir. Dec. 15, 2011) (en banc), *available at* http://www.ca9.uscourts.gov/media/view_subpage.php?pk_id=0000008546. The Government's position was that this would constitute "exceeding authorized access" under Section 1030 provided that the defendant had a prohibited purpose at the time of the access. *Id.* at 14:40. However, the Government conceded that if the defendant obtained the information and decided to sell it later, this would not violate Section 1030. *Id.* at15:14.

[Section 1030] calls for only an objective analysis of whether an individual had sufficient 'authorization.' While a confidentiality agreement or other policies or obligations owed to an employer may prohibit misuse of a company's internal computer system or misappropriation of confidential information therein, the plain text of [Section 1030] does not.").

D. The Rule of Lenity Requires That "Exceeds Authorized Access" Be Read in Its Narrow Sense

43. The Defense submits that the meaning of "exceeds authorized access" is abundantly clear, both by its plain meaning and through an analysis of the legislative history. The Government, however, submits that the accused's purpose in accessing the information in question should be grafted onto Section 1030. Thus, the Government posits that an individual can exceed authorized access by accessing information with a subjective purpose that is inconsistent with the governing use policy or the computer owner's interests. To the extent that there are two possible interpretations of a statute – one broad and one narrow – courts should apply the rule of lenity and adopt the narrow interpretation.

44. It is well established that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *United States v. Carr*, 513 F.3d 1164, 1168 (9th Cir. 2008) (quoting *Rewis v. United States*, 401 U.S. 808, 812 (1971)). The Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants. *See Santos*, 553 U.S. at 514 (2008) (citing *United States v. Bass*, 404 U.S. 336, 347-49 (1971); *McBoyle v. United States*, 283 U.S. 25, 27 (1931); *United States v. Gradwell*, 243 U.S. 476, 485 (1917)). "This venerable rule . . . vindicates the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed." *Id.* Therefore, "[t]he rule of lenity, which is rooted in considerations of notice, requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government." *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006).

45. Military courts have accepted the rule of lenity when construing ambiguous criminal statutes. *See United States v. Schelin*, 15 M.J. 218, 220 (C.M.A. 1983); *United States v. Cartwright*, 13 M.J. 174, 176 & n.4 (C.M.A. 1982); *Inthavong*, 48 M.J. at 630 ("'This policy of lenity means that [courts] will not interpret a federal criminal statute so as to increase the penalty that it places on an individual when such an interpretation can be based on *no more than a guess* as to what Congress intended.' *Ladner v. United States*, 358 U.S. 169, 178, 79 S.Ct. 209, 214, 3 L.Ed.2d 199 (1958) (emphasis added)"); *United States v. Ferguson*, 40 M.J. 823, 830 (N.M.C.M.R. 1994)("'It is an ancient rule of statutory construction that penal statutes should be strictly construed against the government . . . and in favor of the persons on whom penalties are sought to be imposed.' Sutherland Stat Const § 59.03 (5th Ed). A corollary to the rule of strict construction is the 'rule of lenity' whereby ambiguities in penal statutes are resolved in favor of lenity. *Id.* Statutes that declare conduct criminal or laws that expressly define or limit punishments for any offense are classified as penal. *Id.* at § 59.02. The UCMJ is a penal statute. Rule for Courts–Martial (R.C.M.) 201, MCM, United States, 1984. With an eye to *Levy*, we conclude the UCMJ is generally subject to the rule of strict construction and the "rule of lenity." *See United States v. Schelin*, 15 M.J. 218 (C.M.A.1983).").

46. Thus, under the rule of lenity, this Court should adopt the narrow meaning of "exceeds authorized access." That is, one exceeds authorized access when one bypasses technical, computer-based restrictions to access information on the computer than one is not entitled to access. This is exactly what the Ninth Circuit held in *Nosal III*:

> If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly. The rule of lenity requires "penal laws . . . to be construed strictly." *United States v. Wiltberger*, 18 U.S. (5 Wheat.) 76, 95, 5 L.Ed. 37 (1820). "[W]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *Jones* [*v. United States*], 529 U.S. [848,] 858, 120 S.Ct. 1904 [(2000)] (internal quotation marks and citation omitted).
>
> The rule of lenity not only ensures that citizens will have fair notice of the criminal laws, but also that Congress will have fair notice of what conduct its laws criminalize. We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals. "[B]ecause of the seriousness of criminal penalties, and because criminal punishment usually represents the moral condemnation of the community, legislatures and not courts should define criminal activity." *United States v. Bass*, 404 U.S. 336, 348, 92 S.Ct. 515, 30 L.Ed.2d 488 (1971). "If there is any doubt about whether Congress intended [the CFAA] to prohibit the conduct in which [Nosal] engaged, then 'we must choose the interpretation least likely to impose penalties unintended by Congress.'" *United States v. Cabaccang*, 332 F.3d 622, 635 n.22 (9th Cir.2003) (quoting *United States v. Arzate–Nunez*, 18 F.3d 730, 736 (9th Cir.1994)).
>
> This narrower interpretation is also a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking – the circumvention of technological access barriers – not misappropriation of trade secrets – a subject Congress has dealt with elsewhere . . . . Therefore, we hold that "exceeds authorized access" in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*.

2012 WL 1176119, at *7-8 (emphases in original). Applying the rule of lenity and what the Defense submits is the proper understanding of "exceeds authorized access," the Government has failed to state a claim.

E. An Expansive Reading of "Exceeds Authorized Access" Is Unconstitutionally Vague and Would Lead to Absurd Results

47. An expansive interpretation of "exceeds authorized access" that would criminalize persons for violating terms of authorized use puts at least one provision of Section 1030 in constitutional jeopardy. In *Nosal I*, the defendant argued to the three judge panel of the Ninth Circuit that the Government's interpretation would "make criminals out of millions of employees who might use

their computers for personal use, for example, to access their personal email accounts or to check the latest college basketball scores." 642 F.3d at 788. The panel majority rejected this contention, concluding that because Section 1030(a)(4) requires an intent to defraud and an action that furthers the fraud, the defendant's "Orwellian" fear was unfounded. *Id.* at 788-89.

48. The en banc Ninth Circuit, however, was not so dismissive. After all, the term "exceeds authorized access" is included in both Section 1030(a)(4) – the provision at issue in *Nosal* – and Section 1030(a)(2)(C). *See* 18 U.S.C. § 1030(a)(2)(C), (4); *Nosal III*, 2012 WL 1176119, at *3. Thus, an interpretation of "exceeds authorized access" for Section 1030(a)(4) purposes is equally applicable to Section 1030(a)(2)(C). *Nosal III*, 2012 WL 1176119, at *4. Section 1030(a)(2)(C) does not require an intent to defraud like Section 1030(a)(4) does. *See id.* at *3-4. Instead, a person is guilty of a violation of Section 1030(a)(2)(C) when that person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer," 18 U.S.C. § 1030(a)(2)(C), where the term "protected computer" includes a computer connected to the internet. *See Nosal*, 2012 WL 1176119, at *3-4. Therefore, under "the government's proposed interpretation, millions of unsuspecting individuals would find that they are engaging in criminal conduct." *Id.* at *4. The court colorfully elaborated:

> Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes.

Id.

49. The *Nosal III* Court found this situation intolerable for two reasons, both tied to the void-for-vagueness doctrine. First, the Government's interpretation posed serious notice concerns. *See id.* Second, it would "invite arbitrary and discriminatory enforcement." *Id.*

50. The court remarked that "[s]ignificant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read." *Id.* The use of countless websites is governed by a series of private agreements and policies. *Id.* at *5. The prevalence of these agreements and policies is rivaled only by their obscurity to the average person; "most people are only dimly aware of [them] and virtually no one reads or understands [them]." *Id.* If the scant notice of their existence wasn't troublesome enough, "website owners retain the right to change the terms at any time and without notice. Accordingly, behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever." *Id.* at *6 (citation and parenthetical omitted).[12]

[12] The fact that these notice concerns may not be as apparent in this case should be irrelevant to this Court's interpretation of the term "exceeds authorized access." As the en banc *Nosal* Court noted, the interpretation given to the term "exceeds authorized access" is applicable to all provisions of Section 1030 that use some variant of that term. *See Nosal III*, 2012 WL 1176119, at *4 ("Congress obviously meant 'exceeds authorized access' to have the

51. In addition to these substantial notice concerns, the *Nosal III* Court also anticipated that the Government's interpretation would lead to arbitrary and discriminatory enforcement. *See id.* at *4, *6. The Government's assurances of prosecutorial restraint did not satisfy the court:

> The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations. But we shouldn't have to live at the mercy of our local prosecutor. *Cf. United States v. Stevens*, --- U.S. ----, 130 S.Ct. 1577, 1591 (2010) ("We would not uphold an unconstitutional statute merely because the Government promised to use it responsibly."). And it's not clear we *can* trust the government when a tempting target comes along. Take the case of the mom who posed as a 17–year–old boy and cyber-bullied her daughter's classmate. The Justice Department prosecuted her under 18 U.S.C. § 1030(a)(2)(C) for violating MySpace's terms of service, which prohibited lying about identifying information, including age. *See United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). Lying on social media websites is common: People shave years off their age, add inches to their height and drop pounds from their weight. The difference between puffery and prosecution may depend on whether you happen to be someone an AUSA has reason to go after.

Id. at *6 (emphasis in original).

52. Indeed, as the en banc Ninth Circuit indicated, the "Orwellian situation" that was so casually dismissed by the *Nosal I* panel majority actually came to fruition in *Drew*. In that case, the adult defendant created a false MySpace profile of a teenage boy, posted a picture of a teenage boy to that profile without the boy's consent, used that profile to befriend a teenage girl, and eventually used that profile to tell that teenage girl that "the world would be a better place without her in it." *Drew*, 259 F.R.D. at 452. The teenage girl took her own life later that day, and the defendant was soon indicted for felony violations of Section 1030(a)(2)(C) and (c)(2)(B)(ii). *Id.* The defendant was alleged to have exceeded her authorized access to MySpace.com because her act of creating the false profile and the posting of a picture of a teenage boy without the boy's consent violated MySpace's terms of service. *Id.* The jury acquitted the defendant of the felony violations but convicted her on misdemeanor violations of Section 1030(a)(2)(C). *Id.* at 453. The defendant then filed a motion for judgment of acquittal, contending that the violation of the terms of service of an internet provider cannot constitute exceeding authorized access under Section 1030 and, if it did, Section 1030 was unconstitutionally vague. *Id.* at 451.

53. The United States District Court for the Central District of California granted the defendant's motion, concluding that Section 1030(a)(2)(C), as interpreted by the court and as

---

same meaning throughout [S]ection 1030. We must therefore consider how the interpretation we adopt will operate wherever in that section the phrase appears."). Therefore, it is no answer to the constitutional concerns raised by the expansive interpretation of the term "exceeds authorized access" to say that no notice concerns are present in this case. Indeed, the *Nosal* panel majority put forth this flawed, myopic rationale, *see Nosal I*, 642 F.3d at 788-89, and that rationale was soundly rejected by the en banc *Nosal* Court, *see Nosal III*, 2012 WL 1176119, at *3-4. The *Rodriguez* and *John* Courts made the same mistake. *See id.* at *6. Accordingly, in choosing the appropriate interpretation of the term "exceeds authorized access" this Court must consider how the chosen interpretation will affect the other provisions of Section 1030. *See id.* at *4.

applied to the defendant's conduct, was unconstitutionally vague. *Id.* at 464-67. First, the court determined that, as it had interpreted Section 1030, the statute presented serious notice problems: "[T]he language of [S]ection 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that [Section 1030] has 'criminalized breaches of contract' in the context of website terms of service." *Id.* at 464. Second, the court explained that under Section 1030(a)(2)(C)'s "'standardless sweep' . . . federal law enforcement entities would be improperly free 'to pursue their personal predilections'" in selecting which violations to prosecute and which to let go unpunished. *Id.* at 467 (quoting *Kolender v. Lawson*, 461 U.S. 352, 358 (1983)). Accordingly, the court concluded that its broad interpretation of "exceeds authorized access" rendered Section 1030(a)(2)(C) unconstitutionally vague as applied to the defendant's conduct. *Id.* at 464, 467.

54. Under the Government's interpretation in this case, if an accused violates the governing terms of use, he is guilty of a federal offense under Section 1030. As described above, this interpretation raises serious constitutional concerns of vagueness – concerns which can be readily avoided by interpreting the phrase "exceeds authorized access" according to its plain meaning.

F. Academic Commentary Supports the View that "Exceeds Authorized Access" Under Section 1030 Must be Interpreted Narrowly

55. Professor Orin Kerr, one of the country's foremost experts in the area of computer crimes and cyber law, has argued in two separate articles that the term "exceeding authorized access" should not be interpreted so as to allow for an inquiry into whether the accused has violated the computer owner's terms of use. Rather, Section 1030 should only capture whether the user by-passed technical restrictions so as to access information that he was not entitled to access. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1572 (2010) [hereinafter Kerr, *Vagueness Challenges*]; Kerr, *Cybercrime's Scope*, *supra*, at 1649.

56. Kerr notes that several courts have correctly recognized that "an employee who is authorized to access an employer's computer is, well, authorized to use the employer's computer." Kerr, *Vaguenss Challenges*, *supra*, at 1584. Under this interpretation, courts have properly held that misuse of an employer's computer in no way renders the access unauthorized; in fact, the misuse is entirely irrelevant to the "exceeds authorized access" inquiry. *See id.* For Kerr, when access is without authorization or exceeds authorized access must be limited "to access that circumvents restrictions by code." Kerr, *Cybercrime's Scope*, *supra*, at 1649. Kerr has explained this code-based approach as follows:

> When a user circumvents regulation by code, she tricks the computer into giving her greater privileges than she is entitled to receive. This normally can occur in two ways. First, a user can enter the username and password of another user with greater privileges . . . . Second, a user can exploit a design flaw in software that leads the software to grant the user greater privileges[.]

Id. (footnote omitted).

57. He views this narrow interpretation as not only correct, but absolutely essential to the CFAA's vitality: "Only a narrow construction of the statute can save its constitutionality." Kerr, *Vagueness Challenges*, *supra*, at 1572. Kerr reasons that a narrow construction is necessary because a more expansive interpretation, like the one adopted by the *John* and *Rodriguez* courts, would likely render Section 1030 both substantially overbroad and unconstitutionally vague. *See* Kerr, *Cybercrime's Scope*, *supra*, at 1658-59.

58. If "exceeds authorized access" is interpreted to cover a person's violations of a website's terms of service or a person's misuse or misappropriation of information that the person was authorized to access in the first place, the overbreadth doctrine is implicated because Section 1030 would in effect be "granting computer owners the power to criminalize speech, and even mere thoughts." *Id.* at 1658. Kerr provides the following example to illustrate this point:

> [A] pro-life owner of a computer network could insert a paragraph in the Terms of Use agreement allowing only those who express pro-life opinions (or even only those who are pro-life) to use the network. Expressing pro-choice viewpoints would violate the Terms of Use, making the access "without authorization" or "exceeding authorized access" and triggering criminal liability.

Id. at 1658-59. The First Amendment would be seriously offended if the CFAA gave a computer owner the power to "harness the criminal law at his discretion" in this manner. *Id.* at 1658

59. Even more problematic, Kerr argues, an expansive interpretation of "exceeds authorized access" would pose serious vagueness concerns. *See* Kerr, *Vagueness Challenges*, *supra*, at 1562, 1572; Kerr, *Cybercrime's Scope*, *supra*, at 1659. "The CFAA has become so broad, and computers so common, that expansive or uncertain interpretations of unauthorized access . . . would either provide insufficient notice of what is prohibited or fail to provide guidelines for law enforcement in violation of the constitutional requirement of Due Process[.]" Kerr, *Vagueness Challenges*, *supra*, at 1562. If a website's terms of service can limit a user's access, as the court held in *Drew*, the notice problems are readily apparent:

> Few users read the terms of service or terms of use of any of the computers they access, much less all of them, and many restrictions feature ambiguous terms that can be quite difficult to interpret. It is difficult, if not impossible, for a typical user to know for sure whether he is in compliance with all of the contractual restrictions regulating each of the computers he has accessed at any given time. Under the broad contractual theory of authorization, however, any violation of the terms of service or terms of use of any computer a person accesses violates the statutory prohibition on unauthorized access.

Kerr, *Cybercrime's Scope*, *supra*, at 1659. The notice problems are just as serious under the expansive interpretation adopted in *John* and *Rodriguez* where an employee's use of information for personal reasons, or contrary to the interests of the employer, can be considered exceeding authorized access:

> [W]e need to recognize that many employees routinely use protected computers in the course of their day for a tremendously wide range of functions. 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, and 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.

Kerr, *Vagueness Challenges*, *supra*, at 1585.

60. For these reasons, Kerr concludes that "[t]he acts of violating [a website's terms of service] and acting contrary to an employer's interest, without more, should not constitute either an access without authorization or exceeding an authorized access." *Id.* at 1572. Such an interpretation would "create a remarkably broad criminal prohibition that has no connection to the rationales of criminal punishment." Kerr, *Cybercrime's Scope*, *supra*, at 1663.

61. Kerr is by no means alone in advocating the necessity of a narrow interpretation of "exceeds authorized access." Indeed, several other commentators have echoed the same refrain. *See, e.g.*, Thomas E. Booms, Note, *Hacking Into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 Vand. J. Ent. & Tech. L. 543, 570 (2011) (advocating a narrow interpretation because "an employee who has permission to access an employer's computer is authorized to use that computer. It should be irrelevant what the employee does on the computer, because the statute emphasizes access to the computer, not its use. This interpretation is not only supported by the plain meaning of the statute, the CFAA's legislative history, and the rule of lenity, but also allows for a consistent and predictable application of the statute." (footnote omitted)); *id.* at 571 (providing the following analogous example: "If a person is invited into someone's home and steals jewelry while inside, the person has committed a crime – but not burglary – because he has not broken into the home. The fact that the person committed a crime while inside the home does not change the fact that he was given permission to enter."); Garrett D. Urban, Note, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 Wm. & Mary L. Rev. 1369, 1407 (2011) ("A code-based approach [like the one advocated by Kerr] to the amended CFAA would limit expansive liability while still allowing for changes in technology"); Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 Duke L. & Tech. Rev. 12, ¶ 23 (2010), *available at* http://dltr.law.duke.edu/2010/08/26/disloyal-computer-use-and-the-computer-fraud-and-abuse-act-narrowing-the-scope/ ("A narrow definition . . . has the dual benefit of providing a clearer standard and being in accord with the initial spirit and purpose of the CFAA.").

62. Therefore, academic commentary provides even further support for the position that the term "exceeds authorized access" should be interpreted narrowly to only cover situations where a

person accesses information that the person is not authorized to access, regardless of the purposes behind the access.

CONCLUSION

63. The Government in this case has not alleged that PFC Manning "exceeded authorized access" within the proper meaning of Section 1030(a)(1). PFC Manning had access to the relevant SIPRNET computers and was authorized to access every piece of information that he allegedly accessed on the SIPRNET. As such, because the Government has failed to allege that PFC Manning's conduct exceeded his authorized access under Section 1030(a)(1), the specifications alleging violations of Section 1030(a)(1) must be dismissed.

64. Wherefore, in light of the foregoing, the Defense requests this Court dismiss Specifications 13 and 14 of Charge II because the Government has failed to allege that PFC Manning's alleged conduct exceeded authorized access within the meaning of Section 1030(a)(1).

Respectfully submitted,

DAVID EDWARD COOMBS
Civilian Defense Counsel