IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES	)	
	)	**RENEWED 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: 22 June 2012
Fort Myer, VA 22211	)	

RELIEF SOUGHT

1. In light of the Government's newly articulated theory on "exceeds authorized access," PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 907(b)(1)(B), again requests this Court to dismiss Specifications 13 and 14 of Charge II because the Government has failed to permissibly 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).

FACTS

3. Relevant to this motion, PFC Manning is charged with two specifications of knowingly exceeding authorized access to a government computer, in violation of Section 1030(a)(1) and Article 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. § 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, 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.

5. On 10 May 2012, the Defense filed a motion to dismiss Specifications 13 and 14 of Charge II for failure to state an offense. In that motion, as well as in its Reply Motion, the Defense urged this Court to adopt the narrow interpretation of the phrase "exceeds authorized access" – that an accused exceeds authorized access only when he bypasses technical restrictions on access and thereby obtains or alters information he is not authorized to obtain or alter – and to reject the Government's expansive interpretation of that phrase. The Defense argued that because PFC Manning was authorized to access every piece of information that he allegedly accessed, he did not exceed his authorize access under Section 1030(a)(1).

6. The Government finally provided its "definitive" theory for the phrase "exceeds authorized access" in its Response to the Defense Motion. Appellate Exhibit XCI, at 3 & n.1. In a brief moment of uncharacteristic clarity, the Government stated without qualification that "[redacted]." *Id.* at 3. Lest there be any lingering confusion on this point, the Government further clarified its position:

[redacted]

Id. at 3 n.1 (emphasis supplied). In addition to belatedly providing its "definitive" theory on "exceeds authorized access," the Government also stipulated to all of the facts contained in the Defense Motion. *Id.* at 2. At no point in its response did the Government contest that PFC Manning was authorized to access each and every piece of information he allegedly accessed.

7. On 8 June 2012, this Court adopted the narrow definition of "exceeds authorized access" advocated by the Defense. *See* Appellate Exhibit CXXXIX, at 9. Specifically, this Court held that "the term 'exceeds authorized access' is limited to violations of restrictions on *access* to

information, and not restrictions on its 'use'." *Id.* (emphasis in original). At oral argument, this Court explained the proper understanding of "exceeds authorized access" as follows: "the narrow definition would be 'exceeds authorized access' would apply to 'inside hackers', individuals whose initial access to a computer is authorized but who access unauthorized information or files." *See* 8 June 2012 Article 39(a) audio; *see also* Appellate Exhibit CXXXIX, at 7.

8. The Government's "definitive" theory on "exceeds authorized access" did not stay definitive for long. Though entirely absent from the Government's Response (which the Government referred to as the "definitive source clarifying the Government's theory for 'exceeding authorized access,'" Appellate Exhibit XCI, at 3 n.1), a new Government theory made its debut during the oral argument and later in the 802 session. The Government indicated that it would attempt to show that PFC Manning exceeded his authorized access by using a particular unauthorized computer program – Wget – to download information that he was authorized to access onto his computer.[1] *See* 8 June 2012 Article 39(a) audio (CPT Morrow: "There are other considerations in this case, namely, as the evidence will show, the use of an unauthorized program to download information.").

9. Wget is a computer program that retrieves content from web servers, and is part of the GNU Project (a free software, mass collaboration project, announced on September 27, 1983, by Richard Stallman at MIT). Its name is derived from *World Wide Web* and *get*.[2] Although the program was not apparently officially authorized for the individual user, it was authorized for use on the Army Server components of the system. *See* Attachment A. As such, Wget is a program that is authorized to be used on certain military computers. *Id.*

10. Even while hinting at this new theory at the eleventh hour, the Government still did not dispute that PFC Manning was authorized to access all of the information he allegedly accessed.

WITNESSES/EVIDENCE

11. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the previous submissions of the parties. The Defense also requests the Court to consider the following attachments to this motion:

a) Attachment A – email referencing authorization of Wget; and

b) Attachment B – Classified Attachment, Intelink Logs Forensic Report, Bates # 00124331.[3]

---

[1] Consistent with its practice throughout this case, the Government has provided the Defense with the most skeletal version of its theory. Accordingly, the new Government theory articulated above is the Defense's best guess based on the cryptic description provided by the Government. As was the case with the Government's previous "definitive" theory, everyone will have to wait until the Government's Response to this motion reveals the Government's new "definitive theory" *du jour*.

[2] *See* http://en.wikipedia.org/wiki/Wget; *see also* http://www.gnu.org/software/wget/.

[3] The Defense requests that the Government provide a copy of the specific Bates number page for the Court through the Court Security Officer.

LEGAL AUTHORITY AND ARGUMENT

12. The Government's new theory is born of convenience, not of principle. As such, it does not withstand careful scrutiny. PFC Manning's use of an unauthorized program, Wget, to download the information specified in Specification 13 of Charge II does not change and cannot change the only fact that matters in the "exceeds authorized access" inquiry: PFC Manning was authorized to access each and every piece of information he allegedly accessed. The Government is simply wrong in its theory that the use of an unauthorized program to download the information converts what would otherwise be authorized access to that information into "unauthorized access" or "exceeding authorized access." Whether or not PFC Manning used Wget to download the information is of no moment; under the language of Section 1030, as well as this Court's ruling and the great weight of authority, PFC Manning could not have exceeded his authorized access because he was authorized to obtain the information he obtained.

13. Moreover, the Government's "new" argument is simply a variation of its old "definitive" theory. Realizing that the explicit purpose-based restriction was getting it nowhere, the Government fell back on its reliance on the manner in which the information is downloaded – here, through the use of an unauthorized program, Wget – as being determinative of "exceeds authorized access." Both the Government's old theory and its new theory depend heavily on the word "so" in Section 1030(e)(6). That dependency is, for the reasons discussed by the Defense in its initial motion and reply, entirely misplaced. "Exceeds authorized access" is not concerned with the *manner* in which information is downloaded; it is rather concerned with whether the defendant was *authorized to obtain or alter the information* that was obtained or altered. Therefore, the Government's expansive interpretation, in both its old and new formulations, should be definitively laid to rest by this Court.

14. Additionally, the Government's Wget theory does not even cover Specification 14 of Charge II. The forensic evidence relied on by the Government demonstrates that PFC Manning downloaded the information referenced in that Specification directly onto his computer without using Wget.[4] Accordingly, the Government cannot in good faith maintain that its Wget theory covers Specification 14. Therefore, as the Government has not indicated any theory other than its now-rejected explicit purpose-based restriction theory for the information in Specification 14 of Charge II, that specification should be dismissed.

15. Finally, this Court has the power to dismiss a specification where the dispositive issue is capable of resolution without trial on the general issue of guilt. The Government does not dispute that PFC Manning was authorized to access the information that he allegedly accessed. Rather, it has simply offered legal theories as to why his otherwise authorized access exceeded authorized access. The resolution of this legal issue (i.e. whether the Government states a cognizable legal theory of "exceeds authorized access") need not await trial on the general issue of guilt. Such a legal issue is instead the quintessential example of an issue capable of resolution without trial on the issue of guilt.

---

[4] The very purpose of a program like Wget is to download multiple documents in a timely manner. A person would not use Wget to download one document, which can simply be downloaded by clicking "Save As" (or some variation thereof).

16. For these reasons, this Court should dismiss Specifications 13 and 14 of Charge II.

A. A Person Exceeds Authorized Access Only When He Obtains or Alters Information that He is Not Authorized to Obtain or Alter

17. A person "exceeds authorized access" under Section 1030(e)(6) only when he obtains or alters information that he is not authorized to obtain or alter. The language of Section 1030(e)(6), as well as this Court's ruling and the great weight of authority, make this fact abundantly clear. Where, as here, it is determined that the person was authorized to access (i.e. obtain or alter) the information at issue, the "exceeds authorized access" inquiry ends. The extraneous considerations that the Government has relied on with its new and old theories – the manner in which the information is downloaded and the purpose for which the information is accessed or used – are entirely irrelevant to the "exceeds authorized access" inquiry. As the Government does not and cannot dispute that PFC Manning was authorized to access the information specified in Specification 13 of Charge II, that specification must be dismissed for failure to state a cognizable offense.

18. Section 1030(e)(6) defines "exceeds authorized access" as follows: "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). This definition demonstrates that the Computer Fraud and Abuse Act (CFAA) is concerned with the relationship between the accesser and the *information*: is the accesser entitled to obtain or alter the information at issue?

19. This statutory definition is not concerned with the *purposes* for which the accesser obtains or alters the information. It is also not concerned with the *manner* in which the accesser obtains or alters the information. *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."). Rather, the only relevant consideration under the statutory definition of "exceeds authorized access" is whether the accesser was entitled to obtain or alter the information at issue. In this case, it is undisputed that PFC Manning was entitled to access the information. The Government's Wget theory – that PFC Manning exceeded authorized access by using an unauthorized program to download the information – erroneously focuses on the manner in which PFC Manning downloaded the information. But the manner in which he downloaded the information is beside the point, since at all times he remained entitled to access the information in question.

20. The Government's Wget theory is equally inconsistent with the 1996 legislative history of Section 1030, which makes clear that the CFAA targets those who access information that they are not authorized to access. As the report of the Senate Committee on the Judiciary explains, "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." S. Rep. No. 104-357, at 6 (1996) (emphasis supplied). One who accesses information he is entitled to access does not in any way "deliberately break into a computer," *id.*,

regardless of the program used to download the information. Nothing in the 1996 legislative history, or in any of the legislative history of Section 1030, provides an iota of support for the Government's theory that the manner in which information is downloaded is determinative, or even relevant, in the "exceeds authorized access" inquiry.

21. Additionally, the Government's focus on the manner in which the information is downloaded, rather than the authority to access the information, is wholly inconsistent with this Court's formulation of "exceeds authorized access." This Court properly framed the "exceeds authorized access" inquiry at oral argument: "'exceeds authorized access' would apply to 'inside hackers', individuals whose initial access to a computer is authorized but *who access unauthorized information or files*." *See* 8 June 2012 Article 39(a) audio (emphasis supplied); *see also* Appellate Exhibit CXXXIX, at 7. PFC Manning's use of Wget – an unauthorized program on the computer – to download the information at issue did not thereby make his *access to the information* unauthorized.

22. A simple example demonstrates why this is so. Suppose that the only authorized web browser on government computers is Internet Explorer. Suppose further that a Soldier is authorized to access certain diplomatic cables on that computer. If the Soldier used Internet Explorer to access those cables, no one – not even the Government in this case – would characterize the Soldier's actions as "exceeding authorized access." If a Soldier downloaded the web browser Firefox to the Government computer, that browser would be an unauthorized program, since the only authorized browser on the computer is Internet Explorer. Would the Soldier's use of Firefox to obtain those same diplomatic cables make the Soldier's access to those cables unauthorized? Under the Government's Wget theory, the answer would be yes. But this cannot be the case under any sensible interpretation of "exceeds authorized access." Whether he uses Internet Explorer or Firefox, the Soldier would be accessing the same cables and in both cases he would be entitled to access those cables. While the Soldier's installation of an unauthorized program on a government computer may itself be a violation of the computer use policy (and subject the Soldier to punishment under Article 92), the mere installation and use of an unauthorized program to download information cannot change the Soldier's authorization to access the underlying information.

23. So it is here. Under the Government's Wget theory, Wget was an apparently unauthorized program for the individual user. But PFC Manning did not use Wget to "access unauthorized information or files." *See* 8 June 2012 Article 39(a) audio. Rather, he used Wget to download information that he was authorized to access. His authorization to access that information remained unchanged irrespective of the *manner* in which he downloaded the information. Under this Court's proper formulation of the phrase "exceeds authorized access," PFC Manning did not "access unauthorized information or files." *See* 8 June 2012 Article 39(a) audio. Accordingly, he did not "exceed authorized access."

24. Moreover, the great weight of authority provides no support for the Government's argument that the manner in which information is downloaded can determine whether a person "exceeds authorized access." In *United States v. Nosal*, for example, the en banc Ninth Circuit explicitly tied the concept of "exceeds authorized access" to the defendant's authorization to access the particular information at issue: "'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized *information or files*)." 676 F.3d 854, 858 (9th Cir. 2012) (en banc) (second emphasis supplied);

see also Appellate Exhibit CXXXIX, at 7 ("*Nosal III* defines 'exceeds authorized access' to apply to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files." (emphasis in original)). Nothing in the definitive discussion of the narrow interpretation of "exceeds authorized access" in *Nosal* gives any indication that the manner in which a person downloads information has any bearing whatsoever on whether the person is authorized to access that information. Along similar lines, the United States District Court for the Southern District of New York recently 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." *United States v. Aleynikov*, 737 F. Supp. 2d 173, 191-92 (S.D.N.Y. 2010) (emphasis supplied). In *Aleynikov*, as here, the Government did not contest that the defendant was authorized to access the particular information at issue. *See id.* at 191 ("The Government concedes that Aleynikov was authorized to access the source code for the Trading System that he allegedly stole[.]"). The court accordingly granted the defendant's motion to dismiss the CFAA count of the indictment. *Id.* at 194. Likewise, in a very recent Section 1030 prosecution, the United States District Court for the Central District of California found, in light of *Nosal*, that the defendant had not exceeded his authorized access because he was authorized to access the information at issue. *United States v. Zhang*, No. CR-05-00812 RMW, 2012 WL 1932843 (N.D. Cal. May 29, 2012) (finding defendant not guilty of Section 1030(a)(4) and (c)(3)(A) violations because defendant "had 'authorized access' to the Marvell Extranet when he downloaded the information from the Marvell Extranet in March 2005 because he had active log-in credentials at that time.").

25. Several civil cases similarly highlight why the Government's Wget theory cannot be sustained under the narrow interpretation of "exceeds authorized access:" the inquiry is limited to whether the *access to the information* is authorized and is not concerned with the *manner* in which that information is downloaded. *See, e.g.*, *Ajuba Int'l, L.L.C. v. Saharia*, No. 11-12936, 2012 WL 1672713, at *12 (E.D. Mich. May 14, 2012) (holding that "a violation [of the CFAA] for "exceeding authorized access" occurs only where initial access is permitted but the access of *certain information* is not permitted." (emphasis supplied)); *Ryan, LLC v. Evans*, No. 8:12–cv–289–T–30TBM, 2012 WL 1532492, at *5 (M.D. Fla. March 20, 2012) ("Under a narrow reading of the provisions of [Section] 1030, a violation for exceeding authorized access occurs where initial access is permitted but the access of *certain information* is not permitted." (quotations omitted) (emphasis supplied)).; *id.* at *6 ("Given that Evans and Espinosa appear to have had unfettered access to the Ryan computers, *data, information, and emails actually accessed*, with the right to add to, delete from, and upload and download matters therefrom, it is doubtful that their conduct can be brought within the purview of either [Section] 1030(a)(2)(C) or [Section] 1030(a)(4) under the narrow reading of those sections." (emphasis supplied)); *WEC Carolina Energy Solutions, LLC v. Miller*, No. 0:10–cv–2775–CMC, 2011 WL 379458, at *4 (D.S.C. Feb. 3, 2011) ("[L]iability under the CFAA, based on an allegation that an employee exceeded authorized access, depends on whether the employee accessed *information* he was not entitled to access. WEC has not alleged that Miller or Kelley accessed information that they were not "entitled to access." Therefore its allegation falls outside the scope of this portion of the CFAA." (emphasis supplied)); *Nat'l City Bank, N.A. v. Republic Mortgage Home Loans, LLC*, No. C09-1550RSL, 2010 WL 959925, at *3 (W.D. Wash. March 12, 2010) ("A CFAA violation occurs only when an employee accesses *information* that was not within the scope of his or her authorization." (emphasis supplied)); *id.* ("It is undisputed that Westmark was authorized to access, view, and utilize the Excel spreadsheet that forms the heart of plaintiff's CFAA claim

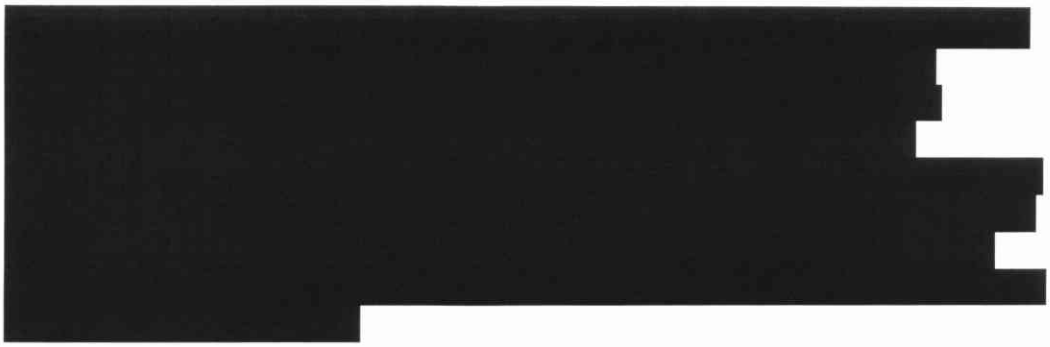
against him. There is no indication that Westmark accessed or obtained any information from National City's computers after he resigned his position with National City. If, as is the case here, the employee were *entitled to access the materials at issue*, nothing in the CFAA suggests that the authorization can be lost or exceeded through post-access conduct. On the other hand, if an employee's access is limited to certain documents, files, or drives, an effort on his part to delve into *computer records to which he is not entitled* could result in liability under the CFAA." (citations omitted) (emphases supplied)); *Lockheed Martin Corp. v. Speed*, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *5 (M.D. Fla. Aug. 1, 2006) ("By applying the plain meaning of the statutory terms to the facts of this case, it is clear that the Employees accessed *with* authorization, did not exceed their authorization, and thus did not violate [Section] 1030(a)(4). The analysis is not a difficult one. Because Lockheed permitted the Employees to access the company computer, they were not without authorization. Further, *because Lockheed permitted the Employees to access the precise information at issue, the Employees did not exceed authorized access*. The Employees fit within the very group that Congress chose not to reach, *i.e.*, those with access authorization. It follows that [Section] 1030(a)(4) cannot reach them. The gist of Lockheed's complaint is aimed not so much at the Employees' improper access of the ATARS information, but rather at the Employees' actions subsequent to their accessing the information. As much as Lockheed might wish it to be so, [Section] 1030(a)(4) does not reach the actions alleged in the Complaint." (emphasis supplied)).

26. In sum, the Government does not dispute that PFC Manning was authorized to access each and every piece of information covered in Specification 13 of Charge II. It instead argues that his use of Wget to download the information specified in Specification 13 renders his otherwise authorized access to that information an excess of his authorization. Such a theory finds no support in Section 1030, its legislative history, and the rulings of this Court and so many others that have adopted the narrow interpretation of "exceeds authorized access." Under that narrow interpretation of the phrase, the only inquiry is whether the accesser is entitled to obtain or alter the information at issue; the manner in which that information is downloaded does not provide an answer to that inquiry. Therefore, since PFC Manning was authorized to access all of the information covered in Specification 13 of Additional Charge II, that specification must be dismissed.

B. The Government's "New" Theory is Simply a Variation of its Already Rejected Expansive Interpretation

27. The Government's "new" theory of "exceeds authorized access" is not really a new one at all; rather, it is a slight tweak of its already rejected expansive interpretation. The explicit purpose-based restriction theory is one formulation of the expansive interpretation of "exceeds authorized access." The Wget theory, focusing as it does on the manner in which information is downloaded, is simply another formulation of this same expansive interpretation. This Court's adoption of the narrow interpretation of "exceeds authorized access" necessarily rejects both formulations of the expansive interpretation. Accordingly, this Court should dismiss the Section 1030(a)(1) specifications.

28. In an attempt to support its explicit purpose-based theory of "exceeding authorized access," the Government Response placed heavy emphasis on the word "so" in Section 1030(e)(6):



Appellate Exhibit XCI, at 4 (emphases in original). The Government hoped that this expansive definition could transform otherwise authorized access to information into exceeding authorized access in some circumstances – namely, when the accesser violated explicit purpose-based restrictions on access. The Government in *Nosal* made a similar desperate attempt to hinge the expansive interpretation of "exceeds authorized access" on this expansive definition of "so:"

> In its reply brief and at oral argument, the government focuses on the word "so" in the same phrase. *See* 18 U.S.C. § 1030(e)(6) ("accesser is not entitled *so* to obtain or alter" (emphasis added)). The government reads "so" to mean "*in that manner*," which it claims must refer to use restrictions.

Nosal, 676 F.3d at 857 (emphasis supplied).

29. Both this Court and the *Nosal* Court, in adopting the narrow interpretation of "exceeds authorized access," rejected this expansive definition of the word "so." The *Nosal* Court rejected this interpretation because it "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id.* This Court reiterated these concerns in its ruling. *See* Appellate Exhibit CXXXIX, at 7 ("The Court, in *Nosal III* at 857, agreed with the appellant's argument and disagreed with the prosecution's attempt to make the CFAA into 'an expansive misappropriation statute' when it was originally created as 'an anti-hacking statute.'").

30. This already-rejected "so" argument is also lingering in the background of the Government's Wget theory on "exceeding authorized access." Although the Government has yet to clearly specify its theory or the legal basis for it, there is simply no way other than the now-discredited "so" argument to get from the language of Section 1030(e)(6), which focuses on the accused's authorization to access *information*, to the Government's Wget theory, which focuses on the *manner* in which the information is downloaded. In other words, under the Wget theory, the Government argues that PFC Manning used an unauthorized program to download information that he was otherwise authorized to obtain. The Government does not dispute that PFC Manning was authorized to access this information. Thus, the only way PFC Manning's access could be unauthorized under the Government's theory is based on his access in these *circumstances*, *see* Appellate Exhibit XCI, at 4, or his access of this information in this particular *manner*, *see* *Nosal*, 676 F.3d at 857 – his use of Wget. Either way, the only way the language of Section 1030(e)(6) would permit such a theory would be if the word "so" had the definition advocated by the Government in *Nosal* and in this case in the Government's Response.

31. Of course, the word "so" in Section 1030(e)(6) does not have that definition. Fortunately, the Defense need not rehash the numerous arguments against the Government's definition of

"so," *see* Appellate Exhibit XC, at 12-13, and Appellate Exhibit XCII, at 2, 4-6, for the matter has already been definitively decided by this Court. In its ruling, this Court adopted the narrow interpretation of "exceeds authorized access" and indicated that it would give instructions "in accordance with the narrow view of *Nosal III*[.]" Appellate Exhibit CXXXIX, at 9. This Court also clearly explained the narrow view of *Nosal*: "*Nosal III* defines 'exceeds authorized access' to apply to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files." *Id.* at 7 (emphasis in original). By rejecting the Government's expansive interpretation and by adopting the narrow interpretation in accordance with *Nosal*, this Court properly rejected the "so" argument once and for all.

32. In the end, the Government's Wget theory is, like the explicit purpose-based theory before it, a theory on use restrictions, not a theory on access restrictions. The Government's Acceptable Use Policy (AUP) perfectly illustrates this fact. The AUP is violated when a user installs an unauthorized program, such as Wget. *See* Appellate Exhibit XCI, Enclosure 6, at 62 ("d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software."). Therefore, as it attempted to do with its explicit purpose-based theory of "exceeds authorized access," the Government is attempting to use a violation of a use restriction under the AUP – the installation and use of Wget – to show that PFC Manning exceeded authorized access. The problem with this effort, then and now, is that "the term 'exceeds authorized access' is limited to violations of restrictions on *access* to information, and not restrictions on its 'use'." Appellate Exhibit CXXXIX, at 9 (emphasis in original). Irrespective of any violation of a use restriction that may have occurred, PFC Manning did not hack into the computer to obtain information he was not authorized to obtain. *See* S. Rep. No. 104-357, at 6 (1996) ("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." (emphasis supplied)); Appellate Exhibit CXXXIX, at 7 ("*Nosal III* defines 'exceeds authorized access' to apply to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files." (emphasis in original)). Instead, PFC Manning was authorized to access every piece of information he obtained.

33. For these reasons, Specification 13 of Charge II must be dismissed.

C. The Evidence Unequivocally Demonstrates that PFC Manning Did Not Use Wget to Obtain the Information Covered by Specification 14 of Charge II

34. Even putting aside the issues with the Government's Wget theory, it only applies to the information covered by Specification 13 of Charge II. It cannot apply to the information covered by Specification 14 of Charge II. Accordingly, as the Government has not articulated any theory other than its now-rejected explicit purpose-based theory for how PFC Manning exceeded his authorized access with respect to this information, Specification 14 of Charge II should be dismissed regardless of the merits of the Government's Wget theory.

35. The forensic evidence indicates that PFC Manning did not use Wget, or any other unauthorized program, to download the information specified in Specification 14 of Charge II. *See* Classified Attachment, Intelink Logs Forensic Report, Bates # 00124331 (forensic report indicating that the keyword "Iceland" was searched for a total of fourteen times from both of PFC Manning's primary and secondary SIPRNET computers). Instead, the forensic evidence

shows that PFC Manning simply downloaded this information directly onto his computer. *Id.* Therefore, as PFC Manning did not use Wget to download the information in Specification 14 of Charge II, the Government's new Wget theory simply cannot apply to this specification.

36. Moreover, the Government apparently has no additional theory on how PFC Manning exceeded his authorized access in obtaining this information, other than its original explicit purpose-based theory. "[T]he Government stated in oral argument that it would present evidence in addition to the AUP." Appellate Exhibit CXXXIX, at 9. The Government has indicated, albeit cryptically, its Wget theory for the information covered by Specification 13 of Charge II. Yet it has offered no additional theory for the information covered by Specification 14 of Charge II. The reason for this glaring omission is obvious: The Government has no additional theory on "exceeds authorized access" for Specification 14. Thus, the only theory of "exceeds authorized access" put forth for Specification 14 is the now-discredited explicit purpose-based theory. The Government therefore has no acceptable theory as to how PFC Manning obtained this information in excess of his authorization, and it does not contest that he was authorized to obtain this information. Accordingly, Specification 14 of Charge II must be dismissed.

D. This Court Has the Authority to Dismiss a Specification When its Underlying Legal Theory is Incorrect

37. This Court does indeed have the power to dismiss a specification where the dispositive issue is capable of resolution without trial on the general issue of guilt. The Government does not dispute that PFC Manning was authorized to access the information that he allegedly accessed. Instead, it has simply offered legal theories as to why his access exceeded authorized access. The resolution of this legal issue (i.e. whether the Government states a cognizable legal theory of "exceeds authorized access") need not await trial on the general issue of guilt. Such a legal issue is instead the quintessential example of an issue capable of resolution without trial.

38. As this Court properly recognized, it has the power to dismiss a specification before the presentation of evidence. *See* Appellate Exhibit CXXXIX, at 9 ("Federal cases dismissing charges before evidence is presented do so under Federal Rule of Criminal Procedure 12. This Court has the power to do the same under R.C.M. 907(b)(1)."). Rule 907(a) provides the standard by which a pretrial motion to dismiss is to be judged: "A motion to dismiss is a request to terminate further proceedings as to one or more charges and specifications on *grounds capable of resolution without trial of the general issue of guilt*." R.C.M. 907(a) (emphasis supplied); *see also* R.C.M. 905("*Any* defense, objection, or *request which is capable of determination without the trial* of the general issue of guilt may be raised before trial." (emphases supplied)). Therefore, where the dispositive issue with the specification is entirely legal (i.e. capable of resolution without trial on the general issue of guilt), a pretrial motion to dismiss is the appropriate vehicle by which to resolve that issue.

39. The issue presented by this motion – whether the Government's theory of "exceeds authorized access" is a permissible one – is just such an issue. The issue is purely one of law: whether a particular theory of proving an essential element of the offense is legally cognizable. The Defense concedes, for the purposes of this motion, the facts alleged by the Government. Additionally, the Government has at no point disputed that PFC Manning was authorized to access all of the information specified in Specifications 13 and 14 of Charge II. The only point of disagreement between the parties is whether the manner in which PFC Manning downloaded

the information in Specification 13 – by using Wget, a program that was not authorized by the AUP – can constitute exceeding authorized access. The Defense submits that if a person is authorized to access certain files, the use of a program like Wget to download those files cannot change the fact that the person is still authorized to access those same files. This is not a factual question which must be resolved after a trial on the general issue of guilt. Instead, this is a purely legal question which is capable of resolution without any further factual development. Therefore, this Court should dismiss Specifications 13 and 14 of Charge II because the Government's legal theory of "exceeds authorized access" is not cognizable. Trial on the general issue of guilt cannot make an uncognizable legal theory a cognizable one.

40. Not only would delaying the inevitable (i.e. the conclusion that the Government cannot show, under any cognizable theory, that PFC Manning exceeded authorized access in accessing this information) until trial serve no useful purpose, an accused would suffer substantial prejudice if the Government was permitted to simply plead the elements of an offense in a specification knowing full well that it would be unable to prove an essential element at trial. To illustrate why this is so, suppose that a Soldier is charged with several crimes – for example, burglary, larceny and sexual assault of a minor. Suppose further that the Government has properly pled the elements of all of these offenses in the specifications, including the element of the sexual assault of a minor offense that the victim is a minor. If the Government has alleged in the specification that "the victim was a minor at the time of the offense" but it knows that the victim was actually nineteen years old at the time of the offense, the Soldier would suffer severe prejudice if that specification was not dismissed pretrial for failure to state an offense. Since the sexual assault of a minor specification alleges all of the essential elements of that offense, it would survive a motion to dismiss for failure to state an offense if military courts did not have the authority to dismiss adequately pled specifications based on impermissible legal theories. The Government would therefore be permitted to fully present its evidence on the sexual assault offense, all the while knowing that the "minority of the victim" element could not be satisfied. Only after the Government has fully presented its case would the Soldier be entitled to a finding of not guilty under R.C.M. 917. At that late stage, the members would have heard all about the conduct underlying the sexual assault offense. Even though the sexual assault of a minor offense would be resolved in the Soldier's favor, the members will still retire to deliberate on the burglary and larceny offenses having heard about the Soldier's conduct on the sexual assault offense. The knowledge of that unsavory conduct may lead the members to find the Soldier guilty on the burglary and larceny offenses because of extraneous, legally irrelevant considerations, such as a desire to punish the Soldier for the conduct underlying the sexual assault offense, notwithstanding the entry of a finding of not guilty on that offense, or a belief that the Soldier has a criminal character and probably committed the other offenses as well. In either case, the motion for a finding of not guilty under R.C.M. 917 cannot protect the Soldier from this danger of prejudice. The only vehicle that would adequately protect the Soldier from this danger would be a vehicle that prevents the Government from fully presenting its case based on an impermissible legal theory as to an essential element of an offense. That vehicle is the motion to dismiss for failure to state an offense under R.C.M. 907(b)(1).

41. This danger of prejudice to the accused is not confined to the hypothetical realm. In this case, PFC Manning is charged with twenty specifications in addition to Specifications 13 and 14 of Charge II. If the Government is permitted to fully present its case on Specifications 13 and 14 when its theory of "exceeds authorized access" is legally insufficient, the Government will be

permitted to put forth evidence that PFC Manning disclosed numerous diplomatic cables. As part of its proof on these offenses, the Government will also adduce evidence that the disclosure of these cables caused, or could have caused, damage to interests of the United States. While this proof is presented, the Government, the Defense, and this Court will all know that the Government's theory of "exceeds authorized access" is legally insufficient. The only group that will not know that the Government's theory is legally insufficient will be the group deciding PFC Manning's guilt or innocence: the court-martial members. While a motion for a finding of not guilty under R.C.M. 917 can ensure that the members do not find PFC Manning guilty of Specifications 13 and 14, it cannot erase from the minds of the jurors the evidence of the disclosure of the cables and the potential damage caused by the disclosure. And it cannot prevent that evidence from influencing – consciously or subconsciously – the members' determination of PFC Manning's guilt or innocence on the remaining twenty specifications. Only a pretrial dismissal for failure to state an offense under R.C.M. 907(b)(1) can prevent the danger of such grave prejudice to PFC Manning.

42. There is an additional reason why a pretrial dismissal under R.C.M. 907(b)(1), and not a motion for a finding of not guilty under R.C.M. 917, should be used to dismiss a properly pled specification based on a legally insufficient theory as to an essential element. In this case, the parties agree that clause 1 and 2 of Article 134 is a lesser-included offense (LIO) of the alleged Section 1030(a)(1) offenses, provided, of course, that the Government's legal theory underlying the Section 1030(a)(1) offenses is cognizable. If PFC Manning is forced to wait until the time for a R.C.M. 917 motion before the legally insufficient Section 1030(a)(1) offenses are resolved in his favor, the Government would get the windfall of a LIO when the original specification was legally defective and should have been dismissed outright. In other words, the Government would be able to prove a derivative offense – the LIO – even though the charged offense does not withstand legal scrutiny. Therefore, in addition to the danger that the members will use the evidence presented on the Section 1030(a)(1) offenses for improper purposes, PFC Manning would be further prejudiced in this regard. To avoid the danger of this prejudice, the Court must exercise its power to dismiss this specification pretrial pursuant to R.C.M. 907(b)(1).

43. For these reasons, this Court does have the power to dismiss a sufficiently pled specification that is premised on a legally insufficient theory as to one essential element of the offense, and this Court should accordingly exercise that power and dismiss Specifications 13 and 14 of Charge II.

CONCLUSION

44. Notwithstanding its last minute shift in theory, the Government has still 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. The Government has not disputed this crucial fact. Accordingly, 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.

45. For these reasons, 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.

Respectfully submitted,

DAVID EDWARD COOMBS
Civilian Defense Counsel