IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES	)	
	)	**DEFENSE REPLY TO**
v.	)	**GOVERNMENT RESPONSE TO**
	)	**RENEWED DEFENSE MOTION**
	)	**TO DISMISS FOR FAILURE TO**
MANNING, Bradley E., PFC	)	**STATE AN OFFENSE:**
U.S. Army, xxx-xx-9504	)	**SPECIFICATIONS 13 AND 14 OF**
Headquarters and Headquarters Company, U.S.	)	**CHARGE II**
Army Garrison, Joint Base Myer-Henderson Hall,	)	
Fort Myer, VA 22211	)	DATED: 11 July 2012

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 still failed to allege that PFC Manning's alleged conduct exceeded authorized access within the meaning of 18 U.S.C. Section 1030(a)(1).

ARGUMENT

2. The Government Response to the Defense Renewed Motion to Dismiss [hereinafter Government Response] clearly demonstrates that the Government's Wget theory on "exceeds authorized access" is simply a red herring; it is being put forth solely to muddy the waters long enough for the Government to present its evidence to the court-martial members. Perhaps the Government hopes to cling to its assortment of impermissible theories of "exceeds authorized access" just long enough to establish a lesser-included offense for Specifications 13 and 14 of Charge II. Perhaps the Government wishes to prove its case with respect to Specifications 13 and 14 in order to increase the likelihood of a guilty verdict on the other specifications. Whatever its motive, the Government cannot escape the fact that it has no cognizable theory of "exceeds authorized access" that can be applied to PFC Manning's conduct.

3. As a factual matter, it is undeniable that PFC Manning was authorized to access the information covered by Specifications 13 and 14. In its Response, the Government coyly states that it did not stipulate to this fact. The Government, however, also avoids disputing this fact, both in its Response and in all other written and oral representations made to this Court. Moreover, the undisputed evidence and the Government's reliance on its novel theories of "exceeds authorized access" make clear that the Government has no evidence that PFC Manning was not authorized to access the information he allegedly accessed. The Government's attempt to manufacture a factual issue where none exists is not only unsupportable; it borders on bad faith.

4. As to the legal merits of the Government's Wget theory, the Government Response confirms what the Defense anticipated in its Renewed Motion: the Wget theory is simply a new and less

persuasive variant of the worn out (and rejected) expansive interpretation of "exceeds authorized access." The Government fails to identify a single case that supports its theory; this is because there is no case that has permitted a section 1030 claim to proceed based on a pure contract-based "Terms of Use" violation. Moreover, its discussion of the *Nosal* dicta, Professor Orin Kerr's commentary, and the 1996 legislative history is disingenuous. Additionally, the Wget theory would lead to undeniably absurd results. Finally, the Government's suggestion that a court instruction can "balance" an impermissible theory and a permissible one and allow the court-marital members to choose which one to accept is utterly senseless.

5. The Government makes no attempt to address the Defense's argument regarding the Government theory underlying Specification 14 of Charge II. Instead, it advocates, in a single sentence, a "wait and see" approach. The obvious problem with this approach is that the Government cannot be permitted to simply fire a barrage of prejudicial evidence at the members and then, after the smoke has cleared, figure out whether a permissible theory of "exceeds authorized access" fits that evidence. Rather, the time to articulate a cognizable legal theory is now. As the Government has repeatedly demonstrated its inability to articulate such a theory for Specification 14, the dismissal of that specification is long overdue.

6. Finally, both the substance and the tenor of the Government Response shows that the Government's true objective is not to attempt to state a cognizable legal theory for "exceeds authorized access," but rather to delay the day of reckoning for its theory (or theories) until after it has put forth its case to the members. For reasons already stated in the Defense Renewed Motion, any such delay would result in severe prejudice to the accused. The Government offers no response to these concerns. The implication of its silence is clear: the Government either has no response or did not bother to come up with one. Either way, this Court, unlike the Government, cannot cavalierly disregard the concerns of prejudice to an accused.

7. For these reasons, this Court should grant the Defense Renewed Motion and should dismiss Specifications 13 and 14 of Charge II.

A. It is Undeniable that PFC Manning Was Authorized to Access the Information in Specifications 13 and 14 of Charge II

8. It is an undeniable fact that PFC Manning was authorized to access the information in Specifications 13 and 14 of Charge II. The Government has never attempted to dispute this fact in any of its representations to this Court. Moreover, the undisputed evidence and the Government's reliance on its novel theories of "exceeds authorized access" make clear that the Government has no evidence that PFC Manning was not authorized to access the information he allegedly accessed. The Government's lack of candor in manufacturing a factual issue where none exists is astonishing.

9. To be clear, this section of the Defense Reply only addresses the issue of whether PFC Manning was authorized to access the information in the first place. It does not deal with the manner in which he allegedly accessed the information or the purposes for which he accessed it. Rather, this section addresses the straightforward question of whether PFC Manning had authority to access the information; in plain terms, was PFC Manning allowed to use his computer to view (i.e. to "obtain" under Section 1030(e)(6)) the information in Specifications 13

and 14 of Charge II? The Government has steadfastly avoided directly answering this question. It has instead jumped immediately to talking about the purposes for which the information was accessed or the precise manner in which the information was downloaded. Since the Government has refused to answer this question, before addressing the merits of the Government's Wget theory, this Reply first demonstrates that PFC Manning was indeed authorized to access the information in question.

10. In its Response, the Government states that "[redacted]." Government Response, at 1. However, the Government conveniently neglects to address the Defense assertion that the Government has not disputed that PFC Manning was authorized to access all of the information at issue. *See* Defense Renewed Motion, at 2. Certainly nothing in the Government's prior Section 1030 filings or representations during oral argument gave any indication that the Government disputed this fact. Even if not stipulating to a fact equates to disputing that fact, which it does not, any attempt to dispute that PFC Manning was authorized to view all of the information in Specifications 13 and 14 of Charge II is belied by the undisputed evidence and by the Government's reliance on its "exceeding authorized access" theories.

11. It is undisputed that the Net Centric Diplomacy Database was on SIPRNET and did not require any password or separate authorization to access. In its 24 May 2012 Response to Defense Motion to Dismiss Specifications 13 and 14 of Charge II for Failure to State an Offense [hereinafter Government Response to First Motion to Dismiss], the Government states that "[redacted]." Government Response to First Motion to Dismiss, at 2. Thus, it is clear that the cables were freely available to anyone with SIPRNET access. It is equally undisputed that CPT Steven Lim directed all of the analysts to look at that database. *See* Government Response to First Motion to Dismiss, Enclosure 3, at 32 & n.152. Therefore, the undisputed evidence demonstrates beyond hope of contradiction that PFC Manning was authorized to access the information.

12. Moreover, the Government's own theories for "exceeds authorized access" make it obvious that the Government has no evidence that PFC Manning was not authorized to access the information contained in Specifications 13 and 14 of Charge II. Its first theory – the now-rejected explicit purpose-based restriction theory – was articulated in the Government's Response to the first Defense Motion to Dismiss as follows: "[redacted]" Government Response to First Motion to Dismiss, at 3. As expected, the Government used its most recent Response to articulate its newest theory: "[redacted]." Government Response, at 3.

13. Both of the Government's theories are telling. If the Government had even a shred of evidence suggesting that PFC Manning was not authorized to access the information in the first place, its theory of "exceeds authorized access" would be uncontroversial: PFC Manning would

have exceeded his authorized access by using his computer to obtain information that he was not entitled to obtain. Of course, the Government has eschewed any reliance on that straightforward theory, and it has focused instead on the purposes for which the information was accessed and the manner in which the information was downloaded. The only conceivable reason why so much ink has already been spilled on the permissibility of these novel theories is that the Government has no evidence that PFC Manning was not authorized to access this information.

14. Indeed, if the Government does have such evidence and nevertheless persists in arguing about the merits of fringe theories of "exceeds authorized access," then the Government has caused considerable delay in PFC Manning's trial through either incompetence or bad faith, dilatory tactics. The Government has at no point indicated that it has any evidence showing that PFC Manning was not allowed to view the information covered by Specifications 13 and 14 of Charge II. The undisputed evidence, the Government's reliance on various "exceeds authorized access" theories, and the Government's refusal to directly rebut the Defense's assertions regarding PFC Manning's authority to access the information all point unwaveringly to the conclusion that PFC Manning was in fact authorized to access the information he accessed.

15. The time for being coy has long past. If candor to the tribunal is anywhere on the Government's radar, the Government will stop skirting this question and come clean to this Court and the Defense.

B. The Government's Wget Theory is Not Permissible Under this Court's Ruling

16. Returning to the merits of the Wget theory, the Government Response clearly shows that the Wget theory is simply a new (and much less compelling) variant of the already rejected expansive interpretation of "exceeds authorized access." Unfortunately, the Government still does not seem to understand the *Nosal* holding or the Court's ruling. If it did, it would never have advanced the argument that it has. The Government says:

Government Response, at 4. Unfortunately for the Government, this is not a "draconian concept" – it is the law. And if the Government needs it "articulated . . . more clearly," the Defense would suggest that it take another look at the Court's ruling and the cases cited by the Defense. *See* Appellate Exhibit CXXXIX, at 6 ("Therefore an analysis of the legislative history of the CFAA and the phrase 'exceeds authorized access' reveals that the statute is not meant to punish those who use a computer for an improper purpose or in violation of the governing terms of use, but rather the statute is designed to criminalize electronic trespassers and computer hackers."); *id.* at 9 (Court adopting *Nosal* view of "exceeds authorized access:" "[the term] applies to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files"); *see also United States v. Aleynikov*, 737 F. Supp. 2d 173, 191 (S.D.N.Y. 2010) (dismissing CFAA indictment where "[t]he Government concedes that Aleynikov was authorized to access the source code for the Trading System that he allegedly stole[.]"); *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."); *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)).

17. In addition to the reasons identified in the Defense Renewed Motion, there are several other reasons to reject the Wget theory. First and foremost, the Government fails to identify a single case that supports its theory. Additionally, the Government uses the language from *Nosal* and

Professor Orin Kerr in a disingenuous attempt to make a violation of the Acceptable Use Policy (AUP) look like the circumvention of security measures. Moreover, the Government's reading of the 1996 legislative history is incorrect. In addition, the Government's Wget theory would lead to absurd results. Finally, the Government's proposed "balance" of an impermissible theory with a permissible one makes no sense.

i) There is Absolutely No Case Law to Support the Government's "New" Theory

18. The Government has not identified a single case lending any support to its theory that the use of an unauthorized program can make otherwise authorized access to information exceeding authorized access. Not one case. The Government apparently requests that this Court become the first in the nation to adopt this particular variation of the expansive interpretation of "exceeds authorized access."

19. There are only three conceivable theories of how an accused can exceed authorized access to a computer. First, the user can exceed non-purpose based contractual restrictions on access. In other words, this involves the computer user violating any of the various contractual "terms of use" that govern computer access aside from those pertaining to the improper or unauthorized use of information (e.g. restrictions on how old you need to be to access a website, restrictions on permissible software/hardware to be used on the computer, etc.). The expressions "terms of use" are also referred to variously in the case law as "terms of service," "terms of access," "acceptable use policy" and the like. Second, the user can exceed purpose-based restrictions on access – whether explicit or implicit.[1] That is, the computer user can use the information obtained from the computer in a way that is contrary to the purposes for which such information is intended to be used. This second scenario is that contemplated in *Nosal, John* and *Rodriguez*. Third, the user can bypass technical restrictions on access (e.g. crack a code; guess at a password, etc.), thereby tricking the computer into giving him greater privileges than he otherwise enjoys.

20. These three scenarios can be seen along a spectrum:

THEORY 1	THEORY 2	THEORY 3
|	|	|
Violating Contractual Terms of Use	Violating Purpose-Based Restrictions On Access	Bypassing Technical Restrictions On Access
LEAST COMPELLING		*MOST COMPELLING*

[1] Implicit limitations exist where there is no governing "Terms of Use" policy which expressly proscribes using the information for purposes for which the authorization does not extend. Rather, by using agency principles, some courts have held that there is an implicit limitation on a computer user's access, such that he loses authorized access once he uses the computer in a manner contrary to the computer owner's interests. *See, e.g. Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) ("Citrin's breach of his duty of loyalty terminated his agency relationship (more precisely, terminated any rights he might have claimed as IAC's agent-he could not by unilaterally terminating any duties he owed his principal gain an advantage) and with it his authority to access the laptop, because the only basis of his authority had been that relationship.").

The further one moves to the left of the spectrum, the less compelling the justification for maintaining a Section 1030 violation. All courts recognize that if facts fall within Theory 3, then a Section 1030 violation is cognizable. Courts are split on Theory 2 – i.e. this is the *Nosal*, *Rodriguez*, and *John* line of cases. No court has ever recognized Theory 1, a pure breach of contract, as supporting a 1030 violation. The Government has moved from Theory 2, which the Court (correctly) found to be an impermissible theory, to Theory 1, a theory which is *far less compelling* than Theory 2. If a Court has held that Theory 2 is not viable, it follows as a matter of law that Theory 1 is not viable.

21. The leading case on Theory 1 is *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), which "raise[d] the issue of whether (and/or when will) violations of an Internet website's terms of service constitute a crime under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. [Section] 1030." *Id.* at 451. Otherwise stated, "[the] central question is whether a computer user's intentional violation of one or more provisions in an Internet website's terms of services (where those terms condition access to and/or use of the website's services upon agreement to and compliance with the terms) satisfies the first element of section 1030(a)(2)(C) [exceeds authorized access]. If the answer to that question is "yes," then seemingly, any and every conscious violation of that website's terms of service will constitute a CFAA misdemeanor." *Id.* at 457.

22. In *Drew*, 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." *Id.* 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.* That is, the defendant violated non-purpose based contractual terms of service. 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.

23. 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 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. … Thus, while "ordinary people" might expect to be exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties." *Id.* at 464.

24. Second, "if a website's terms of service controls what is 'authorized' and what is 'exceeding authorization' – which in turn governs whether an individual's accessing information or services on the website is criminal or not, [S]ection 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will." *Id.* The court further noted that "[i]f *any* violation of *any*

term of service is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but it would, in turn, render the statute incredibly overbroad and contravene the second prong of the void-for-vagueness doctrine as to setting guidelines to govern law enforcement." *Id.* at 464-65.

25. Third, the court noted the very common sense proposition that "by utilizing violations of the terms of service as the basis for the [S]ection 1030(a)(2)(C) crime, that approach makes the website owner-in essence-the party who ultimately defines the criminal conduct." *Id.* at 465. The *Drew* Court concluded that "[t]his will lead to further vagueness problems. The owner's description of a term of service might itself be so vague as to make the visitor or member reasonably unsure of what the term of service covers." *Id.* The court further observed that "website owners can establish terms where either the scope or the application of the provision are to be decided by them *ad hoc* and/or pursuant to undelineated standards. For example, the MSTOS [MySpace Terms of Service] provides that what constitutes 'prohibited content' on the website is determined 'in the sole discretion of MySpace.com[.]" *Id.* The court also expressed concern that the terms of service "may allow the website owner to unilaterally amend and/or add to the terms with minimal notice to users." *Id.*

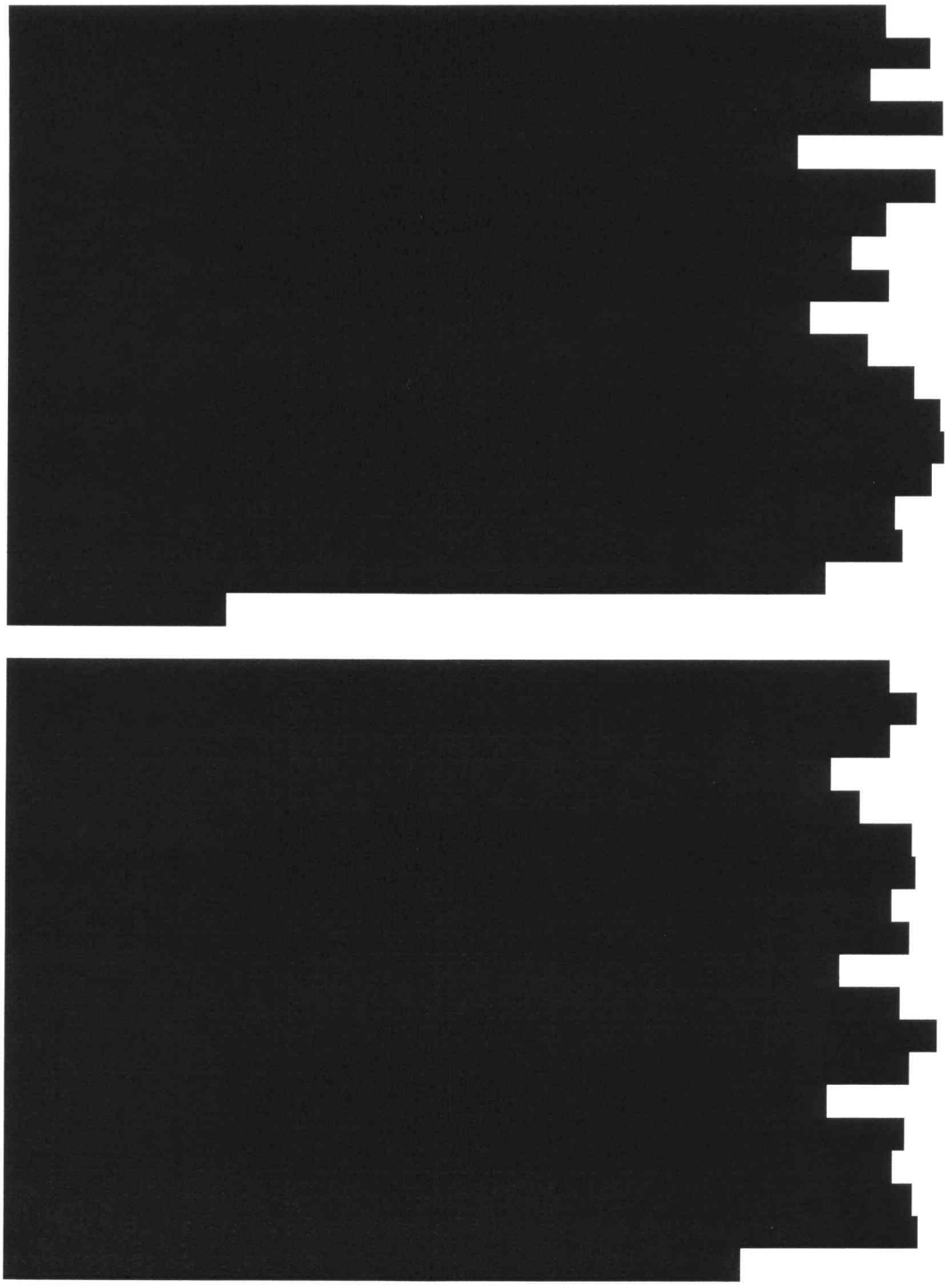
26. Thus, the *Drew* court rejected the possibility that contractual terms of service agreements could provide the factual basis to state a Section 1030 claim. And for good reason. Any lay person can see the danger in allowing the computer owner to unilaterally define by contract the scope of a criminal statute which carries with it the possibility of 10 years in prison. To the Defense's knowledge, no case has ever accepted that non-purpose-based contractual terms of service violations can form the basis for a Section 1030 offense. The Government's "new" theory falls squarely in Theory 1 – PFC Manning exceeded his authorized access because he used an unauthorized program, proscribed by the terms of use, in order to download information. Accordingly, it should be rejected.

ii) The Government is Trying to Confuse the Court By Pretending that PFC Manning Bypassed Technical Restrictions on Access

27. Perhaps because it recognizes that Theory 1 is dead on arrival, the Government is attempting to confuse this Court by arguing that PFC Manning was an "inside hacker" who "circumvent[ed] procedures," "hacked the information," and "bypassed a code-based restriction." Government Response, at 5. In other words, the Government is attempting to make this look like a Theory 3 scenario. This Court should not be fooled by the Government's continued deceit.

28. By affixing these labels to the conduct at issue, the Government is trying to bring PFC Manning's conduct within the *Nosal* holding and Professor Kerr's construct of technical or code-based restrictions (i.e. Theory 3). Unfortunately, the Government is deliberately distorting language to make it look like there was a "circumvention" of technical restrictions, when in reality – as the Government well knows – there was no such thing. In its desperate attempt to keep a non-cognizable specification on the charge sheet, the Government is trying to manipulate this Court into erroneously believing that to use Wget, one would need to "hack" the computer and bypass security restrictions. Nothing could be further from the truth.

29. The Government states:



Government Response, at 5.

30. Thus, the Government appears to concede that an accused can only be brought within the purview of the section if the accused bypassed technical or code-based restrictions on access. The Government cites Professor Kerr twice for this proposition. A look at what Professor Kerr

actually said, however, reveals that the Government could not be more off-the-mark in labeling the use of unauthorized software a code-based restriction. Professor Kerr distinguishes between "regulation by code" and "regulation by contract." Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1644-46 (2003). An easy way of understanding this distinction is that "regulation by code" means that the computer owner has inserted some code (i.e. programming language) into the computer which prevents a user from accessing certain information. *See id.* at 1644-45. Regulation by contract means that the computer owner regulates access to the computer by imposing contractual (usually written) limits on the computer user. *See id.* at 1645-46. It is critically important to understand the difference between the two because Professor Kerr maintains (and the case law uniformly bears out) that courts are only concerned with the former for the purposes of Section 1030.

31. Professor Kerr elaborates on the distinction between "Regulation by Code Versus Regulation by Contract" as follows:

> Although unauthorized access statutes speak of authorization as if it were a monolithic concept, there are in fact two fairly distinct ways in which access or use of a computer can be unauthorized. Each type corresponds to one of the basic ways that a computer owner can regulate a user's privileges. A computer owner can regulate a user's privileges by code or by contract. Similarly, a computer user can engage in computer misuse by circumventing code-based restrictions, or by breaching contract-based restrictions.
>
> When an owner regulates privileges by code, the owner or her agent codes the computers software so that the particular user has a limited set of privileges on the computer. For example, the owner can require every user to have an account with a unique password, and can assign privileges based on the particular account, limiting where the user can go and what she can do on that basis. For a user to exceed privileges imposed by code, the user must somehow "trick" the computer into giving the user greater privileges. I label this approach "regulation by code" because it relies on computer code to create a barrier designed to block the user from exceeding his privileges on the network.
>
> Circumventing regulation by code generally requires a user to engage in one of two types of computer misuse. First, the user may engage in false identification and masquerade as another user who has greater privileges. For example, the user can use another person's password, and trick the computer to grant the user greater privileges that are supposed to be reserved for the true account holder. If A knows B's username and password, A can log in to B's account and see information that B is entitled to see, but A is not.
>
> Alternatively, a user can exploit a weakness in the code within a program to cause the program to malfunction in a way that grants the user greater privileges. Consider a so-called "buffer overflow" attack, a common means of hacking into a computer. A buffer overflow attack overloads the victim computer's memory

> buffer, forcing the computer to malfunction and default to an open position that gives the user "root" or "super user" privileges. These privileges give the user total control over the victim computer: With root privileges, the user can access any account or delete any file. The attack circumvents the code-based restriction that limited the user to her own account. Such misuse violates the intended function test introduced in the Morris case; a user who exploits a weakness in code to trick the victim computer into granting the user extra privileges does so by using the code in a way contrary to its intended function.
>
> The second way an owner may attempt to regulate computer privileges is by contract. The owner can condition use of the computer on a user's agreement to comply with certain rules. If the user has a preexisting relationship with the owner/operator, the conditions may take the form of Terms of Service. If no such relationship exists, the conditions may appear as Terms of Use to the service the computer provides, such as a click-through agreement that might appear prior to use of a website. For example, an adult website may require a user to promise that she is at least eighteen years old before allowing her to access adult materials available through the website. Finally, the restriction may be implicit rather than stated in the written text.
>
> Regulation by contract offers a significantly weaker form of regulation than regulation by code. Regulation by code enforces limits on privileges by actually blocking the user from performing the proscribed act, at least absent circumvention. In contrast, regulation by contract works on the honor system, or perhaps more accurately, the honor system backed by contract law remedies. Consider the adult website that requires users to indicate that they are at least eighteen years old before it allows users to enter. A seventeen-year-old can access the adult website just as easily as an eighteen-year-old can. The only difference is that the seventeen-year-old must misrepresent her age to access the site. To use a physical-world analogy, the difference between regulation by code and regulation by contract resembles the difference between keeping a stranger out by closing and locking the door and keeping a stranger out by putting up a sign in front of an open front door saying "strangers may not enter."

Id. at 1644-46 (footnotes omitted).

32. As is clear from the above passage, the notion of inside hackers who circumvent technical restrictions refers to a user who "somehow 'trick[s]' the computer into giving the user greater privileges." *Id.* at 1644. The reason it is called "regulation by code" is because it relies on *computer code to create a barrier* designed to block the user from exceeding his privileges on the network. *Id.* at 1644-45. That is, "[r]egulation by code enforces limits on privileges by actually blocking the user from performing the proscribed act." *Id.* at 1646. Kerr identifies only two ways that a user can circumvent regulation by code.

33. First,

> the user may engage in false identification and masquerade as another user who has greater privileges. For example, the user can use another person's password, and trick the computer to grant the user greater privileges that are supposed to be reserved for the true account holder. If A knows B's username and password, A can log in to B's account and see information that B is entitled to see, but A is not.

Id. at 1644. There is no evidence the PFC Manning used another user's privileges to gain access to the computer or information in question.

34. Second, "a user can exploit a weakness in the code within a program to cause the program to malfunction in a way that grants the user greater privileges." *Id.* at 1645. Again, there is no evidence that PFC Manning exploited a technical weakness in the code to cause a program to malfunction and thereby obtain greater privileges.

35. These are the exact two code-based restrictions that are highlighted in *Nosal* itself and that are cited by the Government in its Response:

> Suppose an employer keeps certain information in a separate database that can be viewed on a computer screen, but not copied or downloaded. If an employee *circumvents the security measures*, copies the information to a thumb drive and walks out of the building with it in his pocket, he would then have obtained access to information in the computer that he is not "entitled so to obtain." Or, let's say an employee is given full access to the information, provided he logs in with his username and password. In an effort to cover his tracks, he *uses another employee's login to copy information from the database*. Once again, this would be an employee who is authorized to access the information but does so in a manner he was not authorized "so to obtain."

United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012) (en banc) (emphases supplied); *see* Government Response, at 3-4.

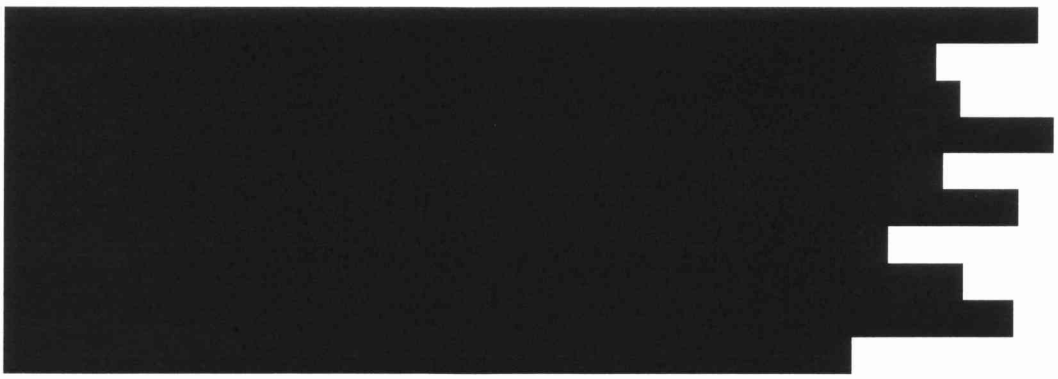
36. The first example in the *Nosal* quote corresponds to Professor Kerr's second code-based limitation, while the second example in the *Nosal* quote corresponds to Professor Kerr's first code-based limitation. The bottom line – whether one looks to *Nosal* or Professor Kerr (who the Defense submits provided the basis for the *Nosal* holding) – is that in order to fall within Section 1030, one must bypass the computer code that creates a barrier between the user and the information in question. If one does not "break" the computer code technical barrier, then one does not exceed authorized access.

37. Apparently, the Government simply does not understand (or is deliberately "misunderstanding") what a code-based restriction is. The Government states, "Thus, the accused violated a restriction on access to the information - he bypassed a code-based restriction - by using Wget to obtain the cables in batches." Government Response, at 5. The passage shows that the Government has no clue what it means to bypass a code-based restriction. It if did, the Government would have specified the "code" (i.e. the computer programming barrier) that PFC Manning allegedly circumvented. The reason it did not, of course, is because PFC

Manning did not need to circumvent a code-based restriction – no such restriction existed.

38. The focus on the circumvention of security measures as the touchstone of "exceeds authorized access" is in perfect harmony with the holdings of *Nosal* and other courts, as well as this Court's ruling and the 1996 legislative history. Both the *Nosal* Court and this Court have held that the term "exceeds authorized access" applies to "inside hackers." *See Nosal*, 676 F.3d at 858 ("'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized *information or files*)." (second 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)); 8 June 2012 Article 39(a) audio ("'exceeds authorized access' would apply to 'inside hackers', individuals whose initial access to a computer is authorized but *who access unauthorized information or files*." (emphasis supplied)); *see also Aleynikov*, 737 F. Supp. 2d at 191-92 ("a person who 'exceeds authorized access' has permission to access the computer, but not the *particular information* on the computer that is at issue." (emphasis supplied)). Like these cited cases, the 1996 legislative history explains the concept of "exceeds authorized access" with reference to a hacker (i.e. one who breaks into a computer to obtain information). *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)).

39. The Government maintains that its theory is consistent with the 1996 legislative history. It is not. The Government states:



Government Response, at 5-6. When Congress notes that "it is the use of the computer that is proscribed" this must be viewed in reference to the concept of electronic trespassing referred to above ("deliberately break into a computer").[2] When one breaks into a computer – whether one is an outside hacker or an inside hacker – one has committed a *crime against the computer*.[3] The use of Wget to download information is not a crime against the computer. It is not electronic trespassing. It is not hacking. It is not circumventing technical or code-based restrictions. Accordingly, nothing about the Government's "new" theory is consistent with the legislative

[2] The Government would prefer if we simply ignored the literal meaning of this language and used it as "[redacted]." It is not the guiding light; it is the test ultimately adopted in *Nosal* and by this Court.

[3] Just as if one has committed a trespass, one has committed a crime against the property.

history.

40. In this case, it is clear – despite the Government's highly disingenuous submission to the contrary – that PFC Manning did not circumvent code-based restrictions to access the information in question. There was no technical code "blocking [PFC Manning] from performing the proscribed act." Kerr, *supra*, at 1646. The Government, however, is hoping that by using Kerr-like language to distort the actual facts, this Court will fall into the trap of believing that the Government has evidence that PFC Manning bypassed technical restrictions. Of course, the Government has no such evidence.

41. Contrary to its assertions, what the Government is actually alleging is a pure contract-based theory (what the Defense calls Theory 1). According to Professor Kerr, the "owner can condition use of the computer on a user's agreement to comply with certain rules. If the user has a preexisting relationship with the owner/operator, the conditions may take the form of Terms of Service." *Id.* at 1645 (footnote omitted). Professor Kerr describes the difference between code-based and contract-based regulation as follows: "Regulation by code enforces limits on privileges by actually blocking the user from performing the proscribed act, at least absent circumvention. In contrast, regulation by contract works on the honor system, or perhaps more accurately, the honor system backed by contract law remedies." *Id.* at 1646. Here, PFC Manning was not permitted to use Wget to download any information on the computer because it was an unauthorized program under the AUP (for which PFC Manning is *already* separately charged under Article 92). This is a textbook example of a contract-based restriction. The only reason PFC Manning could not use Wget was because it was not on a "list" of approved software – not because the Army included code in the computer that prevented PFC Manning from using the software, which he then circumvented.

42. Professor Kerr's real world analogy for this distinction is instructive: "the difference between regulation by code and regulation by contract resembles the difference between keeping a stranger out by closing and locking the door and keeping a stranger out by putting up a sign in front of an open front door saying 'strangers may not enter.'" *Id.* at 1646. In this case, the analogy can be taken one step further. Here, we have the equivalent of a sign that reads "strangers may enter, but they may not enter in a particular manner."

43. The Government has not been forthright with the Court in the past. When asked whether the Government had evidence *aside from the AUP* that PFC Manning had bypassed restrictions on access, the Government said "yes." Audio, Oral Argument; Appellate Exhibit CXXXIX, at 9. It did not. All it has is a different section of *the very same AUP*. This is particularly disheartening because the Court conditioned its ruling upon the Government's misrepresentation that it had evidence "aside from the AUP." Appellate Exhibit CXXXIX, at 9. In short, the Defense submits that the Government took great liberties with the truth – which, in turn, caused the Court to not dismiss charges which should have been dismissed. In this respect, the Defense submits that the Government had once again demonstrated a lack of candor with the Court.

44. As if that weren't enough, the Government is not being forthright with the Court once again. Rather than properly conceding that PFC Manning did not bypass technical restrictions (i.e. there was no code-based computer security gate that PFC Manning had to circumvent to use Wget), the Government is purposely warping language in order to keep a fatally defective specification

alive. The Government, of course, has distorted language in the past.[4] It is doing so again. The Government is trying desperately to use all the right words ("circumvent[ed] procedures," "hacked the information," and "bypassed a code-based restriction") so that it can pull the wool over this Court's eyes. It cannot be permitted to do this.

45. Under no stretch of the imagination can the Government's Wget theory be squared with this Court's adoption of the narrow interpretation of "exceeds authorized access." The Government's new theory hinges on the use of an unauthorized program to perform what would otherwise be authorized tasks. The obligation to refrain from using unauthorized programs is created by the AUP. *See* Government Response to First Motion to Dismiss, 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."). The Government, spurned in its first attempt to make a violation of one provision of the AUP "exceeding authorized access," has now simply picked a different provision of the same AUP for its "new" theory. In short, the Government has proceeded under Theory 1, even though it tries to dress it up as Theory 3. Since no court has ever allowed Theory 1 to proceed, and because Theory 1 provides an even less compelling rationale than Theory 2 (which has already been rejected by the Court), the specifications must be dismissed.

iii) The Government's "New" Theory Leads to Even More Absurd Results than Its Previous "Definitive" Theory

46. The Government's "new" theory leads to even more absurd results than its prior "definitive" theory. To illustrate this point, imagine PFC Manning used Excel 2009 to export (i.e. download) the information in Specifications 13 and 14 of Charge II. Imagine further that Excel 2009 was an authorized program and that the 2009 version of Excel was the only version of Excel authorized to be used on his government computer. Even under the Government's new theory, his conduct would not constitute "exceeds authorized access," since the Government cannot dispute that PFC Manning was allowed to view (i.e. authorized to obtain) this information. *See* Part A, *supra.* However, if PFC Manning had updated the version of Excel on his computer to Excel 2010 – an unauthorized version of Excel – and had downloaded the exact same information in the exact same way, he would have "exceeded authorized access" under the Government's new theory. Thus, the Government's theory would make ten years imprisonment based on the exact same conduct hinge solely on which version of Excel PFC Manning used. *See* 18 U.S.C. § 1030(c)(1)(A) (providing for a maximum of ten years imprisonment for a violation of Section 1030(a)(1)); *see also* Defense Renewed Motion, at 6 (providing a similar example using Internet Explorer and Firefox). Further, if PFC Manning used Excel 2010 to download all the cables for use in his job (i.e. he did not disclose the cables to unauthorized persons), he could still be subject to criminal prosecution under Section 1030. *See* 18 U.S.C. § 1030(a)(2)(C) (requiring only that the defendant "exceed authorized access" and obtain information from a protected computer).

47. Moreover, the Government's new theory is not limited to mere violations of this particular provision of the AUP. Conceivably, any violation of the AUP would render a user's access to

[4] Recall the Government indicating: a) that it was "unaware" of forensic results; b) that ONCIX did not have an interim or a final damage assessment; c) that there was a distinction between "investigation" and "damage assessment;" d) that the DOS has not "completed" a damage assessment, etc.

information unauthorized in the Government's view. *See Drew*, 259 F.R.D. at 464-65 ("[I]f a website's terms of service controls what is 'authorized' and what is 'exceeding authorization' – which in turn governs whether an individual's accessing information or services on the website is criminal or not, section 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will. If *any* violation of *any* term of service is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but it would, in turn, render the statute incredibly overbroad and contravene the second prong of the void-for-vagueness doctrine as to setting guidelines to govern law enforcement.").

48. The Government argues that "[redacted]" Government Response, at 5 (emphasis supplied). It fails to recognize, however, that *any* violation of the AUP would bypass the "ordinary method," *id.*, of accessing information on a government computer, since the AUP itself sets forth the ordinary method of accessing information.

49. The very next line of the AUP after the requirement that computer users not install or use unauthorized software requires the use of virus-checking procedures before a user accesses information from certain sources. *See* Government Response to First Motion to Dismiss, Enclosure 6, at 62 ("e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk."). Would failure to use virus-checking procedures before accessing information from a system constitute exceeding authorized access? Not under any sensible interpretation of that term. But under the Government's theory, such a failure would constitute exceeding authorized access because it would bypass the "ordinary method of accessing information" as defined in the AUP. Government Response, at 5. And such a failure alone would, under the Government's view, subject a user to conviction and up to a year imprisonment under Section 1030(a)(2)(C). *See* 18 U.S.C. § 1030(a)(2)(C) (requiring only that the defendant "exceed authorized access" and obtain information from a protected computer);[5] *id.* § 1030(c)(2)(A) (providing punishment for a violation of Section 1030(a)(2)); *Nosal*, 676 F.3d 859 (explaining that interpretation of "exceeds authorized access" chosen by the Court must apply to all provisions of Section 1030 using that phrase).

50. Similarly, the provision of the AUP that precedes the requirement that computer users not install or use unauthorized software provides that computer users must have secure passwords. *See* Government Response to Defense Motion to Dismiss, Enclosure 6, at 62 ("c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use user ID, common names, birthdays, phone numbers. military acronyms, call signs, or dictionary words as passwords or pass-phrases.")). Would failure to use a sufficiently secure password (e.g. BradleyManning1234) mean that a user

[5] To "obtain information" includes merely reading information. *See Drew*, 259 F.R.D. at 457 ("As also stated in Senate Report No. 104-357, at 7 (1996), *reprinted at* 1996 WL 492169 (henceforth "S.Rep. No. 104-357"), "... the term 'obtaining information' includes merely reading it.")

would exceed authorized access when he then logged onto the computer? Again, under the Government's theory, the answer would be yes. There is no logical basis for distinguishing between the various contractual restrictions on computer access/use. Any and all violations of restrictions outlined in the AUP would be punishable criminally.

51. Moreover, there is no requirement that any of the restrictions be reasonable. If the Army wanted to, it could write into the AUP that "Every soldier, prior to accessing a U.S. Army computer, must sing the national anthem." *See* Government Response to First Motion to Dismiss, Enclosure 6, AR25-2, B-2 ("Army organizations may tailor the information in the sample AUP to meet their specific needs, as appropriate."). A failure to sing the national anthem prior to accessing the computer would then subject the soldier to jail time.

52. One need not be Oliver Wendell Holmes to see that the Government's theory is flat out preposterous. It simply replaces one variation of the expansive interpretation of the phrase "exceeds authorized access" (based on a violation of one provision of the AUP) with another variation of that same expansive interpretation (based on a different provision of the same AUP). However, the Government's theory now is even more ludicrous because it does not depend on a purpose-based limitation on access. A violation of any contractual term of access/use/service would be a violation of Section 1030.

53. The Government cannot sensibly explain how this new theory can be reconciled with this Court's adoption of the narrow interpretation of the phrase "exceeds authorized access." Indeed, it is beyond comprehension how the Government can still pursue in good faith any theory of "exceeds authorized access" based on a violation of the AUP after this Court definitely held 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); *see also id.* at 6 ("Therefore an analysis of the legislative history of the CFAA and the phrase 'exceeds authorized access' reveals that the statute is not meant to punish those who use a computer for an improper purpose *or in violation of the governing terms of use*, but rather the statute is designed to criminalize electronic trespassers and computer hackers.").

iv) The Court is Not Permitted to "Balance" Legal Theories: Either an Offense is Cognizable or it is Not

54. Finally, the Government's argument that its proposed instruction balances the competing theories of the Government and the Defense makes no sense. Perhaps in denial, the Government refuses to acknowledge that its expansive purpose-based restriction theory was definitely rejected by this Court. As explained in this Reply and in the Renewed Defense Motion, the Government's Wget theory is even more impermissible than its purpose-based restriction theory. An impermissible theory cannot be "balanced" with a permissible theory in a jury instruction, so that the members decide which legal theory to accept. The members do not decide the proper interpretation of a statute.

55. For these reasons and the reasons articulated in the Defense Renewed Motion, this Court should reject the Government's plea for a revival of the expansive interpretation and should accordingly dismiss Specifications 13 and 14 of Charge II.

C. The Government Has Offered No Permissible Theory for Specification 14 of Charge II

56. The Government does not even try to address the Defense's argument regarding the Government theory underlying Specification 14 of Charge II. Instead, it endorses an impermissible "wait and see" approach. However, the time to articulate a cognizable legal theory is now, not at the close of evidence. The reason it has not done so is obvious: it does not have a cognizable legal theory. As such, Specification 14 must be dismissed.

57. The Defense Renewed Motion clearly explained that the forensic evidence unequivocally established that PFC Manning did not use Wget to obtain the information in Specification 14 of Charge II. *See* Defense Renewed Motion, at 10-11. Since the only theory articulated by the Government that could therefore be applied to Specification 14 was its now-rejected explicit purpose-based theory, the Defense Renewed Motion argued that Specification 14 should be dismissed.

58. The Government responded to the Defense's contentions in the last sentence of its Response. It stated that "[redacted]" Government Response, at 7. This is no response at all.

59. For one thing, the Government has things backwards. While it may prefer to just present its Section 1030 case without putting much thought into its theory of "exceeds authorized access" for Specification 14 of Charge II, the prejudice concerns to PFC Manning identified in the Defense Renewed Motion preclude the Government from doing so. *See* Defense Renewed Motion, at 11-13. The Government's theory cannot be dependent upon this Court's instructions; rather, this Court's instructions must be dependent on the Government's theory, provided it can articulate a cognizable one.

60. For too long, the Government has refused to fully articulate its theory or theories for "exceeds authorized access." When asked as part of the bill of particulars motion what its legal theory was for section 1030, the Government refused to provide an answer. The Government finally did articulate its "definitive" theory in its first Response. Once it lost that motion, the Government's "definitive" theory gave way to cryptic indications that it had other evidence and theories. And after all this, the Government continues to be cagey with its theory for Specification 14. The time to speak is now. Either it has a cognizable legal theory for Specification 14 of Charge II or it does not. If it does not, it should just say so and stop the delay that results from its meritless arguments to the contrary.

D. This Court Should Put an End to the Government's Delay Tactics

61. Both the substance and the tenor of the Government Response shows that the Government's true objective is not to attempt to state a cognizable legal theory for "exceeds authorized access," but rather to delay the day of reckoning for its theory (or theories) until after it has put forth its case to the members. For reasons already stated in the Defense Renewed Motion, any such delay would result in severe prejudice to the accused. The Government offers absolutely no response to these concerns – perhaps because it knows that its tactics are indeed deliberately designed to

cause prejudice to the accused. This Court, unlike the Government, does not have the luxury of so blithely disregarding the concerns of prejudice to an accused.

62. The Defense Renewed Motion put forth several prejudice concerns that would arise if the Government is given a free pass on articulating a cognizable legal theory until after the evidence has been presented. *See* Defense Renewed Motion, at 11-13. Those concerns need not be reproduced here.

63. In its Response, the Government offers no rebuttal to these prejudice concerns. Instead, the Government, without even acknowledging these concerns, requests in the alternative that this Court "[redacted]." Government Response, at 7. The Government's decision to avoid responding to the prejudice concerns is telling; either the Government deemed these concerns too insubstantial to even warrant a response or too insurmountable to even attempt one. Either way, the Government, through its silence, seeks to sweep these prejudice concerns under the rug, hoping that this Court will overlook them just as the Government has done.

64. Of course, this Court cannot treat these prejudice concerns as dismissively as the Government has treated them. There can be no deferment on the issue of whether the Government has a cognizable theory of "exceeds authorized access." No matter how much the Government may wish it were otherwise, a cognizable legal theory is a prerequisite to the presentation of even a single piece of evidence on the Section 1030 specifications. The Government has been challenged to come forward with a permissible theory for "exceeds authorized access." It has yet to do so. It cannot now request that the Court wait to see what the evidence bears out. Given the history of the Government's conduct in both the Section 1030 motions and argument and other aspects of this case, the Government is not entitled to the benefit of the doubt that such a "wait and see" approach would give it. Even if it were so entitled, deferment of this issue until after presentation of the Government's evidence would result in irreversible prejudice to PFC Manning. *See* Renewed Defense Motion, at 11-13. This Court should not permit the Government to delay this matter any longer.

E. The Government's Response to this Motion is the Latest in a Long List of Instances Where the Government has not been Candid with the Court

65. As may be apparent from recent motions practice, the Defense is increasingly troubled by the Government's lack of candor. We have seen the lack of candor play out particularly in recent discovery dispute. However, we have also seen this elsewhere (e.g. in the Article 104 motion and the motion for a bill of particulars). It is time for the Government to begin taking its ethical responsibilities as officers of the Court more seriously.

66. Here, the facts are not in dispute – however, the Government is making it look like they are. The uncontroverted facts are these:

- Anyone with SIPRNET access had access to the diplomatic cables on the Net-Centric Diplomacy database;
- There were no password restrictions on the Net-Centric Diplomacy database;
- Any and all diplomatic cables could be downloaded by anyone with SIPRNET access;

- There were no restrictions (either technical or contract-based) on the quantity of cables that could be downloaded from the Net-Centric Diplomacy database;
- There were no technical restrictions that electronically blocked users from employing Wget, or any type of authorized or unauthorized software, from downloading cables from the Net-Centric Diplomacy database.

67. Thus, there are three basic questions that the Government continually dances around in an effort to fabricate a factual issue:

> *Question One: Did PFC Manning have permission to view the diplomatic cables on the SIPRNET?* The answer here is "yes." The Government, in an effort to confuse the Court, states that it did not stipulate to this fact. It doesn't need to. There is no factual question that all persons who had SIPRNET access had access to the diplomatic cables.
>
> *Question Two*: *Did PFC Manning have permission to download the diplomatic cables?* Again, the answer here is "yes." As the Government states, PFC Manning was permitted to download the diplomatic cables – though under the AUP, he should have used an authorized program.
>
> *Question Three: Did PFC Manning have to bypass a technical code-based restriction (i.e. some sort of electronic gate) to download the cables using Wget?* The answer here is "no." There was no code or programming in the computer that physically prevented a user from employing an unauthorized program (Wget or otherwise) to download the information. The source of the restriction on using Wget is found solely in the contractual terms of use.[6]

68. If the Government were honest with itself – and more importantly with the Court – it would admit the truth of the aforementioned. Its continued obfuscation, in keeping with its motions practice in the rest of the case, far exceeds the outer boundaries of zealous advocacy.

69. Not only has the Government continued to play hide the ball with clearly undisputed facts, it has also played hide the ball with the Court as to the evidence it has in its possession. This Court's denial of the Defense Motion to Dismiss Specifications 13 and 14 of Charge II was based solely on the Government's representations that it had evidence aside from the AUP. In denying the Defense Motion, this Court explained:

> Whether the Court should dismiss the Specifications before presentation of evidence depends on whether the issue is capable of resolution without trial on the issue of guilt. In this case, the Government stated in oral argument that it would *present evidence in addition to the AUP*. The Court does not find that the issue is capable of resolution prior to presentation of the evidence.

---

[6] One might add a fourth question: *Is there evidence that PFC Manning used Wget with respect to the cable in Specification 14*? The answer is clearly "no." However, the Defense submits that the answer to that question is actually irrelevant because even if PFC Manning had used Wget with respect to the information in Specification 14, this would still not state a cognizable section 1030 offense.

Appellate Exhibit, CXXXIX, at 9 (emphasis supplied). Well, what is the Government's evidence "in addition" to the AUP? There is no such evidence. At the very least, the Government, instead of waiting idly by for a renewed motion to dismiss from the Defense, should have alerted the Court to the fact that the "new evidence" is simply a different section of the *same AUP*.

CONCLUSION

70. For the reasons articulated above and in the Renewed Defense Motion, the Defense requests this Court to dismiss Specifications 13 and 14 of Charge II because the Government has still failed to allege that PFC Manning's alleged conduct exceeded authorized access.

Respectfully submitted,

DAVID EDWARD COOMBS
Civilian Defense Counsel