

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Prosecution Notification  
to the Court:  
GAL Evidence

19 July 2013

On 18 July 2013, the Court ordered the United States to set forth admitted evidence related to a user's authorization to download or remove information from the United States Forces-Iraq Microsoft Outlook/SharePoint Exchange Server global address list (hereinafter "GAL"). In accordance with the Court's order, the United States proffers the following.

Army Regulation 25-2 (hereinafter "AR 25-2") defines an information system as a "[s]et of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information." Prosecution Exhibit (hereinafter "PE") 93 at 86-87.<sup>1</sup> AR 25-2 adds that this "includes [Army Information System] applications, enclaves, outsourced IT-based processes, and platform IT interconnections." *Id.* The GAL collects, stores, and processes military information. *See* Testimony of CW4 Nixon; Testimony of CW4 Rouillard. The GAL is an information system under AR 25-2.

AR 25-2 prohibits Soldiers from using an employee-owned information system for classified or sensitive information. PE 93 at 47 (citing AR 25-2 ¶ 4-31(a)). Furthermore, "[t]he use of an [employee-owned information system] for ad-hoc (one-time or infrequent) processing of unclassified information is restricted and only permitted with [Information Assurance Manager], [Designated Approving Authority], or commander approval." *Id.* (citing AR 25-2 ¶ 4-31(b)). COL Miller testified that the accused was not authorized to engage in the charged misconduct, to include the asportation of records and United States government information to WikiLeaks. *See* Testimony of COL Miller.

AR 25-2 defines sensitive information as "[a]ny information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. § 552(a) (The Privacy Act). . . ." PE 93 at 21 (citing AR 25-2 ¶ 4-4(b)(2)) (emphasis added); PE 93 at 98 (citing AR 25-2 definition of sensitive information); *see also* AR 530-1 ¶ 1-5(c) (defining sensitive information to include, *inter alia* information related to names, unit assignment, or organizations); AR 530-1 ¶ 2-1 (stating that Soldiers will protect from disclosure sensitive information to which they have access). Sensitive information includes, *inter alia*, "information in routine DOD payroll, finances, logistics, and personnel management systems." PE 93 at 92. This list is non-exhaustive. *See id.* AR 25-2 also mandates that "[a]ll Army personnel" will "protect and restrict access to all documentation . . . describing IS architectures,

<sup>1</sup> PE 93 is a copy of AR 25-2. The page numbers cited in this filing correspond to the page numbers printed in AR 25-2, not the electronic page numbers of the .pdf.

designs, configurations, vulnerabilities, address listings, or user information.” PE 93 at 38 (citing AR 25-2 ¶ 4-13(a)).

The loss or misuse of the information in the GAL could affect or harm the privacy of listed Servicemembers. *See* Testimony of CW4 Nixon. The GAL contained personally identifiable information. *See* Testimony of CW4 Nixon; Testimony of CW4 Rouillard; Testimony of Mr. Lewis. The GAL operates as a “phonebook” for a user. *See* Testimony of CW4 Nixon. The GAL identified, *inter alia*, a user’s name, username, domain, alias addresses, certificates, unit, and phone numbers. *Id.*; *see* PE 47; PE 48; PE 147(a); PE 148(b). This information also revealed organizational structure. *See* Testimony of CW4 Rouillard. The GAL and its contents were not available to the public and were available only to authorized personnel. *See* Testimony of CW4 Nixon; Testimony of CW4 Rouillard. In 2010, a user did not have the capability to export the GAL from the server onto an authorized NIPR computer. Testimony of CW4 Nixon.

The loss or misuse of the information in the GAL could affect or harm military operations and system security. *See* Testimony of CW4 Rouillard; Testimony of CW4 Nixon. Adversarial forces value and seek the GAL and its contents. *See* Testimony of CW4 Rouillard; Testimony of Mr. Lewis. The GAL reveals user names, which increases the ability of a malicious actor to compromise United States computer systems. *See* Testimony of CW4 Rouillard. Accordingly, a malicious actor could use the GAL for spear phishing attacks to compromise United States computer systems. *Id.* The GAL further reveals network architecture, *see* Testimony of CW4 Rouillard, thereby aiding an adversary’s offensive operations against United States computer systems. *See* PE 93 at 38 (citing AR 25-2 ¶ 4-13(a)); *see also* PE 93 at 22 (citing AR 25-2 ¶ 3-3(c)(5) (mandating protection of system and network integrity)). Additionally, the GAL could be used as part of a social engineering attack against Soldiers. *See* Testimony of CW4 Rouillard. Thus, the information in the GAL was sensitive and protected under AR 25-2 ¶ 4-31(a).

The accused’s commander did not authorize the exfiltration of the GAL. *See* Testimony of COL Miller. Moreover, AR 25-2 prohibits downloading the GAL to a NIPR computer and moving it to a personal computer. *See* Testimony of CW4 Rouillard (stating that AR 25-2 prohibits downloading the GAL to a personal computer and that the ability to do an act on a computer system does not mean the act is authorized); PE 93, *supra*. The accused had no reason to download the GAL to his personal computer because he could only send emails from his NIPR computer. *See* Testimony of CW4 Nixon. Therefore, AR 25-2’s prohibition on using a personal computer for sensitive information applied to the GAL and its contents. *See* PE 93, *supra*; *cf.* AR 25-1 ¶ 6-1(d)(1) (4 December 2008) (limiting use of United States Government systems “to the conduct of official business or another authorized use”); PE 93 at 22 (citing AR 25-2 ¶ 3-3(c)(4)-(5) (stating that users must protect information systems located in their respective areas and take no actions that “threaten the integrity of the system or network”)); PE 93 at 28 (citing AR 25-2 ¶ 4-5(a)(7) (prohibiting transfer or possession of information without proper authority)).

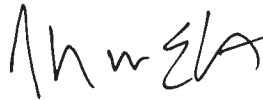
In the time period when the accused extracted the GAL, WikiLeaks published a tweet requesting “.mil email addresses.” PE 31. Extracts of 74,000 email accounts from the GAL

were found on the accused's computer. *See* Testimony of Special Agent Williamson; Testimony of Special Agent Johnson; Testimony of CW4 Nixon (identifying Servicemember names and email accounts in PE 47 and PE 48 as originating from the GAL). The accused created a tasker to describe his mission to "acquire and exfiltrate" the GAL. The accused's tasker defines the purpose as "[t]o e-mail classified messages from USF-I's CIDNE event log from 2004 to 2009." This purpose suggests the tasker was used for previous compromises of sensitive information and that accused's mission regarding the GAL was conducted with the same intent. Consequently, where AR 25-2 prohibited the accused from placing the sensitive information on his personal computer, the accused completed his crime when he completed the prohibited act with a criminal intent.



ALEXANDER VON ELTEN  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel, via electronic mail, on 19 July 2013.



ALEXANDER VON ELTEN  
CPT, JA  
Assistant Trial Counsel