

**UNITED STATES NAVY-MARINE CORPS
COURT OF CRIMINAL APPEALS
WASHINGTON, D.C.**

**Before
C.L. REISMEIER, J.K. CARBERRY, B.L. PAYTON-O'BRIEN
Appellate Military Judges**

UNITED STATES OF AMERICA

v.

**AARON L. BOWLES
CHIEF ELECTRICIAN'S MATE (E-7), U.S. NAVY**

**NMCCA 201100010
GENERAL COURT-MARTIAL**

Sentence Adjudged: 16 September 2010.

Military Judge: CAPT Moira D. Modzelewski, JAGC, USN.

Convening Authority: Commander, Navy Region Mid-Atlantic,
Norfolk, VA.

Staff Judge Advocate's Recommendation: CDR F.D. Hutchison,
JAGC, USN.

For Appellant: LT Ryan Santicola, JAGC, USN; LT Toren G.
Mushovic, JAGC, USN.

For Appellee: LT Ritesh K. Srivastava, JAGC, USN.

31 October 2011

OPINION OF THE COURT

**THIS OPINION DOES NOT SERVE AS BINDING PRECEDENT, BUT MAY BE CITED AS
PERSUASIVE AUTHORITY UNDER NMCCA RULE OF PRACTICE AND PROCEDURE 18.2.**

PER CURIAM:

A general court-martial composed of officers and enlisted members convicted the appellant, contrary to his pleas, of four specifications of possessing media containing images of child pornography in violation of Article 134 of the Uniform Code of

Military Justice, 10 U.S.C. § 934.¹ The appellant was sentenced to six months confinement, three months of hard labor without confinement, reduction to pay grade E-3, and a dishonorable discharge. The convening authority disapproved the sentence of hard labor without confinement, but otherwise approved the sentence as adjudged.

The appellant raises a single assignment of error on appeal: that the military judge erred by admitting evidence obtained from the appellant's external hard drive.

Upon review of the record of trial and the parties' pleadings, we conclude that the sentence and the findings are correct in law and fact, and there was no error materially prejudicial to the substantial rights of the appellant. Arts. 59(a) and 66(c), UCMJ.

Facts

In April 2009, personnel from Naval Information Operations Command (NIOC) inspected USS FORT MCHENRY's computer network. NIOC reports to Naval Network Warfare Command (NETWARCOM) and is charged with conducting onboard "vulnerability assessments" of Navy vessel computer systems. Vulnerability assessments are routine and typically occur semiannually between deployments. The purpose of a vulnerability assessment is to check for intrusions into a computer network from any outside source, and to test for weaknesses in the local network infrastructure that may make it vulnerable to such intrusions. This particular vulnerability assessment was conducted by three NIOC members known as the Blue Team. The Blue Team's inspection proceeded as follows: first, it tested for "unpatched" software, that is, areas where the network was particularly susceptible to encroachment; next, the Team looked for infected files that may have been inadvertently downloaded by crew members (these files often come in the form of games, videos, and images); finally, the Team examined the infections themselves to see what types of viruses had been imported into the network.

On 30 April 2009, after running scans for several days, the Blue Team detected significant vulnerabilities in the USS FORT MCHENRY's network, including one workstation with three infected files from peer-to-peer downloads. The Blue Team highlighted this workstation when providing its overall synopsis that the USS FORT MCHENRY was the "worst unit" it inspected. The

¹ The military judge conditionally dismissed Specification 1 under Charge II as multiplicitous with Specification 6 for findings. Record at 545.

potential for damage from these vulnerabilities was so great, that NIOC had NETWARCOM remove the USS FORT MCHENRY from the Department of the Navy's computer network altogether. NIOC ordered the Blue Team to isolate the workstation in question, perform further testing, and take corrective measures. The Blue Team dispatched one of the USS FORT MCHENRY's information technicians (ITs) to retrieve the hard drive affiliated with the offending workstation. The IT went to the workstation and did not find a hard drive connected to the computer, but did find one in an adjacent desk drawer. She brought it back to the Blue Team for analysis.

The hard drive was the appellant's personal property. The IT who retrieved it knew that the appellant often connected his own hard drive to the USS FORT MCHENRY's network, but she did not know whether this specific hard drive was the appellant's. The Blue Team conducted its examination and found evidence of child pornography. Naval Criminal Investigative Service agents were notified. They interviewed the appellant, who was identified as the workstation's primary user, and he admitted to searching for and downloading child pornography.

In a pretrial Article 39(a), UCMJ, session, the parties litigated the issue of whether the evidence obtained from the appellant's hard drive, along with all subsequently obtained derivative evidence, should be suppressed as the result of a Fourth Amendment violation. The military judge found that the Blue Team performed a MILITARY RULE OF EVIDENCE 313, MANUAL FOR COURTS-MARTIAL, UNITED STATES (2008 ed.), inspection, not a Fourth Amendment search, and denied the defense's motion.

Discussion

The appellant claims that the evidence obtained from the appellant's external hard drive was impermissibly obtained and should have been suppressed. First, the appellant argues that the Blue Team exceeded the inspection's legitimate scope by examining an unconnected hard drive that could not have posed a threat when it was removed from the appellant's workstation. Because the Blue Team's conduct could no longer be properly considered an inspection within the meaning of MIL. R. EVID. 313, it graduated to a Fourth Amendment search. Second, this search was unreasonable because the appellant had a legitimate expectation of privacy concerning the hard drive and its contents. Finally, not only should the hard drive contents have been suppressed, but under the "fruits of the poisonous tree" doctrine, all derivative evidence should have been suppressed as

well, including the appellant's admissions that he searched for and downloaded child pornography, as they were obtained only because investigators were able to confront him with knowledge that he possessed child pornography.

We review a military judge's evidentiary ruling for an abuse of discretion. *United States v. Owens*, 51 M.J. 204, 209 (C.A.A.F. 1999). We will overturn that ruling if the findings of fact are clearly erroneous or unsupported by the factual record, or if the ruling was influenced by an erroneous view of the law. *Id.* See also *United States v. Sullivan*, 42 M.J. 360, 363 (C.A.A.F. 1995). A military judge's conclusions of law are reviewed *de novo*. *Owens*, 51 M.J. 209.

The Fourth Amendment's protections apply to service members. See, e.g., *United States v. Middleton*, 10 M.J. 123, 126-27 (C.M.A. 1981). However, the protections afforded to service members are not identical to those afforded to civilians, because the service member's reasonable expectation of privacy has been balanced to accommodate national security and military necessity. Military commanders are responsible for these imperatives and they may order inspections and inventories to pursue them. In an electronic age, the commander's inspection does not just include physical infrastructure and personnel readiness, but computer systems as well. The extent of the harm caused by a network breach cannot be overstated; crucial components of vessel operability, including communications and combat systems can be impacted. Evidence obtained in the course of a commander's inspection - defined in relevant part by MIL. R. EVID. 313 as an examination the primary purpose of which is to determine and ensure the security of a unit, organization, or vessel - may be admissible at trial.

The threshold question in our analysis concerns the primary purpose of the Blue Team's examination. The military judge made a factual finding that "[t]he Blue Team's purpose in inspecting the workstation for the infected files was in no way a quest for evidence of a crime." Appellate Exhibit LXXXI at 5. This finding was supported by the testimony of Cryptologic Technician Second Class (CTN2) Christopher Kroner, Chief Information Systems Technician Horace Wint, and Information Systems Technician Second Class Colleen Barrett, and it was not contradicted by any evidence presented by the defense. The appellant argues that the hard drive did not pose a threat to network security because it was in a drawer and not plugged in. We disagree. CTN2 Kroner explained that the hard drive had infected and could continuously re-infect the network system if

and when it was reconnected. As the appellant commonly attached his external hard drive to USS FORT MCHENRY's computer network and stored the device in a USS FORT MCHENRY workstation, it was certainly within the purview of USS FORT MCHENRY's commanding officer to make the device subject to NIOC's vulnerability assessment.

The appellant cites *United States v. Conklin*, 63 M.J. 333 (C.A.A.F. 2006), for the proposition that a routine inspection may transform into a Fourth Amendment search if Government agents exceed the scope of the inspection. The appellant in *Conklin* was a trainee living in a dormitory room. His room was subject to random inspections for the stated purpose of ensuring neatness, orderliness, and maintenance in compliance with rules and regulations. While inspecting the appellant's desk, an inspector accidentally disturbed the computer keyboard causing the computer's "wallpaper" to appear and display pornography. The inspector immediately sought assistance from a supervisor, who in turn conducted a more thorough search of various folders on the appellant's hard drive and eventually found evidence of child pornography. CAAF held that the Government could not rely on MIL. R. EVID. 313 to support admissibility of the child pornography because the scope of the inspection was limited to neatness, orderliness, and maintenance in compliance with rules and regulations; the Government's in-depth search exceeded what was needed for these objectives.

Conklin is not applicable to these facts. *Conklin's* analysis began with the stated purpose of the inspection and went on to consider how the Government's conduct deviated from that stated purpose. We do not see a similar deviation in this case. The Blue Team's in-depth examination of the appellant's external hard drive did not exceed its stated purpose and strictly conformed to the inspection's aim of searching for and eliminating network vulnerabilities. The Blue Team was not engaged in a quest for criminal evidence. Its responsibilities were not discharged simply because the appellant's hard drive was unplugged at the time it was retrieved - as evidenced by the testimony of CTN2 Kroner. We therefore conclude that the military judge did not abuse her discretion by finding that the Blue Team's vulnerability assessment qualified as an inspection within the meaning of MIL. R. EVID. 313. Her ruling was not clearly erroneous, it was supported by the factual record, and it was not influenced by an erroneous view of the law.

Because we are convinced that the images from the appellant's computer were obtained in the course of an

inspection and not a Fourth Amendment search, we do not reach the question of whether the appellant had a legitimate expectation of privacy in his workstation desk drawer or external hard drive. And because there was no constitutional violation, we do not reach the question of whether the appellant's confession should have been suppressed as the fruits of an illegal search.

Conclusion

We affirm the findings and the sentence as approved by the convening authority.

For the Court

R.H. TROIDL
Clerk of Court