

**IN THE U.S. NAVY-MARINE CORPS COURT OF CRIMINAL APPEALS
WASHINGTON NAVY YARD
WASHINGTON, D.C.**

BEFORE

C.A. PRICE

E.B. HEALEY

R.C. HARRIS

UNITED STATES

v.

**Jeffrey S. OHNESORGE
Sergeant (E-5), U.S. Marine Corps**

NMCCA 200100199

PUBLISH

Decided 18 February 2005

Sentence adjudged 17 September 1999. Military Judge: R.J. Kreichelt. Review pursuant to Article 66(c), UCMJ, of General Court-Martial convened by Commander, Marine Forces Reserve, New Orleans, LA.

Capt PHILLIP D. SANCHEZ, USMC, Appellate Defense Counsel
CDR BRENT G. FILBERT, JAGC, USNR, Appellate Defense Counsel
CDR GEORGE F. REILLY, JAGC, USN, Appellate Defense Counsel
LT FRANK L. GATTO, JAGC, USNR, Appellate Government Counsel

PRICE, Senior Judge:

Contrary to his pleas, the appellant was convicted of violation of a lawful general regulation by using his government computer to download images of nude men, women, and children, in violation of Article 92, Uniform Code of Military Justice, 10 U.S.C. § 892. A general court-martial comprised of officer members sentenced the appellant to reduction to pay grade E-1 and a bad-conduct discharge. The convening authority approved the sentence as adjudged.

The appellant contends that: (1) the evidence is legally and factually insufficient; (2) the military judge erred in denying a motion to suppress computer subscriber information; (3) the military judge erred in allowing the Government to reopen its case-in-chief; and, (4) the military judge erred in refusing to allow the defense to offer exculpatory evidence.

We have carefully considered the record of trial, the assignments of error, and the Government's response. We conclude that the findings and sentence are correct in law and fact and

that no error materially prejudicial to the substantial rights of the appellant was committed. Arts. 59(a) and 66(c), UCMJ.

Background

The appellant was the Information Systems Coordinator (ISC) in the G-6 section of 4th Marine Division. As such, he was responsible for all hardware and software support of computer systems in the division. He was widely acknowledged as an expert in these areas and enjoyed an excellent reputation among his co-workers.

On 8 September 1998, Master Gunnery Sergeant (MGySgt) Bacher, a drilling reservist, was using the appellant's government computer for official business (a common practice in the division spaces) when he inadvertently discovered adult and child pornography on the computer's hard drive. The images were stored in the G drive/download file. The G drive was a password-protected shared drive accessible through other computers on the network. Subsequent investigation revealed that the images had been downloaded from an Internet site named EasyNews.com, specifically newsgroups such as sex.preteen and sex.teens.

When notified of this discovery, Major (Maj) Bell, the Division G-6, and Maj Wayman, the Inspector-Instructor for Headquarters Battalion, called the appellant in for questioning about the pornography. Also present were MGySgt Bacher and Master Sergeant Daily, the Senior Enlisted Adviser. Maj Wayman advised the appellant that he was suspected of having child pornography on his computer and read him his rights. The appellant indicated he understood his rights.

The appellant initially responded that he didn't know anything about it and denied putting such material on his computer. He mentioned that several co-workers had his password for this shared drive and demonstrated on Maj Wayman's computer how a person could access the shared drive. Then, after some hesitation, the appellant admitted the material was his. Maj Wayman asked him why he had the material, to which the appellant responded that he had a business on the side, apparently for selling the images. However, the appellant soon retracted the statement about the business.

About three weeks earlier, the appellant had purchased an account with EasyNews.com. Mr. Jeff Minor, President of El Dorado Sales, Inc. (El Dorado), testified that his company operated EasyNews.com. He explained that this internet site brings together in one place all news groups on the internet and provides access to binary files such as music, movies, videos, and various images, ranging from "company graphics to NASA pictures, pornography...." Record at 462.

A person could subscribe to EasyNews.com by accessing the web site, registering a user name and password, and providing a

credit card number. The company maintained subscriber information on file, i.e., name, e-mail address and credit card number. When the appellant purchased his account with EasyNews.com, he registered a user name of RuhRowRagy and provided his email address of RuhRowRagy@AOL.com. Using his government computer, the appellant subsequently downloaded numerous pornographic images from EasyNews.com through RuhRowRagy@AOL.com.

Motion to Suppress Computer Subscriber Information

The appellant contends that the military judge erred by denying a defense motion to suppress the appellant's EasyNews.com subscriber information. We disagree.

Litigation of the motion included testimony by Mr. Minor and by Ms. Judith Coulter, a Special Agent (SA) for the U.S. Customs Service. SA Coulter visited the business offices of El Dorado on 16 April 1999 as part of an ongoing Customs Service investigation of possible internet distribution of child pornography through the EasyNews.com website. That investigation was unrelated to the appellant. Before the visit, the staff judge advocate (SJA) for the convening authority contacted SA Coulter and apprised her of a pending Naval Criminal Investigative Service (NCIS) investigation into the appellant's pornography on his government computer. The SJA also told SA Coulter that the NCIS investigation found that one of the user names linked to the appellant was "RuhRowRagy@AOL.com."

During her visit to El Dorado, SA Coulter asked if EasyNews.com had a subscriber with that user name, then assured Mr. Minor that she would provide him with an administrative summons or subpoena for that information. Mr. Minor asked her to call and verify that such a summons would be forthcoming. SA Coulter did so. SA Coulter did not have a summons, subpoena or search warrant at the time. Mr. Minor then searched the subscriber database and found the RuhRowRagy@AOL account. He told SA Coulter that a Jeff Ohnesorge had used that America Online (AOL) account to subscribe to EasyNews.com and also provided SA Coulter with the service activation date and the credit card number used to pay for the subscription. SA Coulter relayed this subscriber information to the SJA and NCIS.

About two weeks later, SA Coulter served a Customs Service administrative summons on Mr. Minor requesting all subscriber information for the account associated with "RuhRowRagy@AOL.com." In response to the summons, Mr. Minor did not provide any additional data. On 8 June 1999, the trial counsel issued a subpoena to EasyNews.com requesting the same subscriber information, along with subscriber information for another screen name and for appellant's full legal name. Records provided in response to the subpoena indicate that the appellant purchased an account with EasyNews.com on 14 August 1998 and maintained the

account for about two months, a period corresponding to the time frame alleged in the specification. The appellant's subscriber information for EasyNews.com was ultimately admitted into evidence during the Government's case-in-chief.

The appellant asserts that SA Coulter's request for subscriber information constituted a search under the Fourth Amendment, that he had a reasonable expectation of privacy in that subscriber information, and that absent a warrant or similar authority, SA Coulter's obtaining of the subscriber information violated his Fourth Amendment rights and his rights under the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2711 and MILITARY RULE OF EVIDENCE 311, MANUAL FOR COURTS-MARTIAL, UNITED STATES (1998 ed.). The Government contends that the appellant did not have a reasonable expectation of privacy in the subscriber information.

The Fourth Amendment extends to the contents of a person's private computer. *United States v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F. 1996). Whether a person has a Fourth Amendment reasonable expectation of privacy in communications from one's private computer depends upon the nature of the communication. *Id.*

In this case, we must decide whether the appellant's subscriber information provided to a commercial Internet site had Fourth Amendment protection. This appears to be an issue of first impression in military jurisprudence. In ruling against the appellant, the military judge cited no military case law. Neither brief cites any military case law on point, and we have not found any. However, two cases from our superior court address related issues and provide helpful guidance.

In *Maxwell*, the court held that a subscriber to an Internet service provider (ISP), in that case AOL, had a reasonable expectation of privacy in the content of electronic mail (e-mail). While the decision did not address subscriber information held by AOL, the court did suggest that there was no reasonable expectation of privacy in AOL records pertaining to Maxwell's account. *Maxwell*, 45 M.J. at 418 ("So far as the company's records are concerned, there is no reasonable expectation that the records are private, and the customer has no control whatsoever over which employees may see the records.")(citation omitted).

In *United States v. Allen*, 53 M.J. 402, 409 (C.A.A.F. 2000), the court held that company data identifying the date, time, user and detailed internet address of sites accessed by Allen may be released without a warrant under the ECPA. The court also noted that even if the ECPA is violated by disclosure of the contents of subscriber e-mail or similar private communications, the ECPA does not list exclusionary rule relief among its various statutory remedies. *Id.* Citing *United States v. Hambrick*, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999), with approval, the court noted

that its analysis did not extend to the type of subscriber information at issue in *Hambrick*.

In *Hambrick*, a state police officer obtained subscriber information similar to that involved in this case by presenting a subpoena to Hambrick's ISP. The subpoena was later ruled to be legally invalid. Thus, the court had to decide whether, in the absence of a valid subpoena or other legal authority, the Fourth Amendment protected the subscriber information. Specifically, the court examined whether or not Hambrick had a reasonable expectation of privacy in the subscriber information. One of the factors cited by the court was that nothing prevented the ISP from disclosing the subscriber information to non-governmental third parties, such as to marketing firms and other similar business concerns. Another factor was that Hambrick knowingly and voluntarily provided the subscriber information to the ISP without any assurance of confidentiality. Ultimately, the court concluded that Hambrick had no reasonable expectation of privacy in his subscriber information.

Considering these cases, and based on our review of the record, we conclude that the military judge did not abuse his discretion in refusing to suppress the subscriber information. Even if the appellant held a subjective expectation of privacy in his subscriber information, which is not supported by the record, there are three reasons why such an expectation would be objectively unreasonable.

The first reason is the nature of the subscriber information. As our superior court suggested in *Maxwell*, there is a difference in the content of private communications and the means by which those communications are authorized, i.e., subscriber information. This is particularly true given the fact that "the credit card information provided, including the account number, card type (VISA), and issuing bank is posted by EasyNews.com through a third party company for verification and payment processing." Military Judge's Ruling on Motion to Suppress of 3 Sep 1999, Appellate Exhibit IX. Thus, subscriber information in this case was not treated as confidential, and there is nothing in the record to indicate that the appellant or any other prospective subscriber might reasonably consider it to be confidential.

The second reason is the nature of the agreement that the appellant had with EasyNews.com. When he applied for a subscription, the appellant was required to consent to the following:

Customer understands that the system is public and not private. Customers agrees that EasyNews has the right to monitor the system electronically from time to time and to disclose any information as necessary to satisfy any law, regulation or other government request, to

operate the system properly, or to protect itself or its users.

Appellate Exhibit IV. Thus, any reasonable prospective subscriber was on notice that EasyNews.com could disclose subscriber information to third parties.

The third reason is the congressional intent manifest in the provisions of the ECPA: "[A] provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to [,] or customer of [,] such service . . . to any person other than a government entity." 18 U.S.C. § 2703(c)(1)(A)(1999).¹ From this, a reasonable person would conclude that subscriber information was not protected from third-party disclosure. For these reasons, we hold that the appellant did not have a reasonable expectation of privacy in the information he voluntarily provided to El Dorado to purchase his account. See *Hambrick*, 55 F.Supp.2d at 508-09; *United States v. Kennedy*, 81 F.Supp.2d 1103, 1110 (D. Kan. 2000).

Even if we were to conclude that the appellant had a reasonable expectation of privacy that was violated by SA Coulter's obtaining of the subscriber information, we hold that the information would have inevitably been discovered through a search authorization or warrant. See *Nix v. Williams*, 467 U.S. 431 (1984); *Maxwell*, 45 M.J. at 422-23.

Legal and Factual Sufficiency of Evidence

The appellant asserts that the evidence is legally and factually insufficient. We disagree.

This court's standard of review for sufficiency of the evidence is set forth in Article 66(c), UCMJ:

(c) In a case referred to it, the Court of Criminal Appeals may act only with respect to the findings and sentence as approved by the convening authority. It may affirm only such findings of guilty, and the sentence or such part or amount of the sentence, as it finds correct in law and fact and determines, on the basis of the entire record, should be approved. In considering the record, it may weigh the evidence, judge the credibility of witnesses, and determine

¹ We note that after the trial concluded and the convening authority approved the sentence, the USA Patriot Act of 2001 amended this section of the statute. That 2001 amendment substantially changed the content of the section. We also note that the amendment expires on December 31, 2005, subject to certain savings provisions. Considering the foregoing, we decline to address the relevance of this section of the statute for other similar cases.

controverted questions of fact, recognizing that the trial court saw and heard the witnesses.

Further, this standard and its application have been recognized and defined by the Court of Appeals for the Armed Forces:

[U]nder Article 66(c) of the Uniform Code, 10 U.S.C. § 866(c), the Court of [Criminal Appeals] has the duty of determining not only the legal sufficiency of the evidence but also its factual sufficiency. The test for the former is whether, considering the evidence in the light most favorable to the prosecution, a reasonable factfinder could have found all the essential elements beyond a reasonable doubt. *Jackson v. Virginia*, 443 U.S. 307 [](1979). For factual sufficiency, the test is whether, after weighing the evidence in the record of trial and making allowances for not having personally observed the witnesses, the members of the Court of [Criminal Appeals] are themselves convinced of the appellant's guilt beyond a reasonable doubt.

United States v. Turner, 25 M.J. 324, 324-25 (C.M.A. 1987).

We hold that a reasonable factfinder could have found, beyond a reasonable doubt, that the appellant committed the charged offense. Moreover, upon careful consideration of the evidence, we are convinced beyond a reasonable doubt that the appellant is guilty of that offense.

Conclusion

We have considered the remaining assignments of error and find them lacking in merit. Accordingly, the findings and the sentence, as approved by the convening authority, are affirmed.

Judge HEALEY and Judge HARRIS concur.

For the Court

R.H. TROIDL
Clerk of Court