UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. YE SANG WANG, Defendant.	Case No. 19-cr-1895-BAS **ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE (ECF No. 92)**

Defendant Ye Sang Wang brings a Motion to Suppress all documents seized from her computer including emails between her and her husband and all evidence obtained as a result of this seizure. (ECF No. 92.) The Government opposes (ECF Nos. 94, 95), and Defendant replies (ECF No. 100). For the reasons stated below, the Court **DENIES** Defendant's Motion.

I. BACKGROUND[1]

Defendant worked for the Department of Defense (DoD) as a logistics specialist for the Navy. She was responsible for purchasing military equipment for Special Reconnaissance Team I (SRT-I). As such she had a classified security clearance.

[1] The summary below is taken from both Defendant's Motion as well as the Government's Response. Unless otherwise indicated, there appears to be no disagreement between the parties as to the underlying facts.

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

Defendant and her husband, Shaohua Wang, were both naturalized U.S. citizens, originally from the People's Republic of China (PRC).

On April 3, 2017, an SRT-I member informed the Naval Criminal Investigative Service (NCIS) that Defendant had attempted to gain a top secret security clearance without the need for one and had travelled to the PRC. NCIS investigated, but subsequently closed the investigation. NCIS did not access Defendant's emails or computer at that time.

On March 6, 2018, an SRT-I Special Security Officer contacted a Counterintelligence Support Officer (CISO)—again noting Defendant's repeated inquiries into obtaining a top security clearance. Additionally, the Officer expressed concerns about Defendant compiling a list of future Naval Special Warfare (NSW) Command deployment personnel records, including names and addresses. The CISO accessed and reviewed Defendant's military email account and computer on March 8, 2018, to assess whether she had violated operational security by transmitting a list of NSW deployment records.

When Defendant was issued a computer for work, she signed a User Agreement (ECF No. 92, Exh.1) in which she consented to the following conditions for her use of the government computer:

(1) "The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, . . . personnel misconduct, law enforcement, and counterintelligence investigations."

(2) "At any time, the U.S. Government may inspect and seize data stored on this information system."

(3) "Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception and search and may be disclosed or used for any U.S. Government authorized purpose."

(4) The security measures—such as the access card and PIN number for the computer—are installed "to protect U.S. Government interests—not for your personal benefit or privacy."

> (5) Nonetheless, consent to this interception, monitoring, inspection and seizing of data "does not negate any applicable privilege" such as attorney-client, psychotherapist-patient or clergy-penitent. However, users are strongly encouraged to seek personal legal counsel before using the information system to communicate something the individual believes to be privileged. And "[u]sers should take reasonable steps to identify such communications or data that the user asserts are protected by such privilege or confidentiality."

(*Id.*)

To provide a reminder to the users of the conditions they agreed to in this User Agreement, a warning banner appeared on all DoD computers when they were powered up, essentially repeating all the conditions of consent that a user agreed to when using the government-issued computer. (ECF No. 95, Exhs. 1 and 2.)

According to the Government, when the CISO reviewed Defendant's military email account, he discovered emails between Defendant and her husband that suggested she was pricing military export-controlled items for sale to individuals in countries, such as the PRC, without a license. Additionally, the CISO found communications that suggested Defendant was using her position as a Logistics Supply Officer to obtain pricing information for export-controlled items. Defendant communicated via email with Scott Larson at Airborne Systems. His response included a warning that the information he was providing was confidential and not to be disclosed. She promptly forwarded the email to her husband.

Again, according to the Government, the CISO further found that Defendant used her military email to request quotes for military equipment, changing her address at the last minute from her SRT-I Command address to a personal address. The communications resulted in companies shipping restricted products intended for U.S. military to recipients that would normally have required additional verification.

Finally, NCIS located an Excel spreadsheet on the computer, in Mandarin, with pages of lists of military devices and gear with associated website URL links and a resume for her husband listing him as founder and manager of "5-Star Surplus."

Discovery of these emails and documents on Defendant's military computer led to search warrants and eventually to indictments against both Defendant and her husband. (ECF No. 1.) Defendant's husband pled guilty to conspiracy to export defense articles without a license and to export defense articles to an embargoed country and money laundering. (ECF Nos. 47, 50.) Defendant faces charges for conspiracy to export defense articles without a license, export defense articles to an embargoed country and commit theft of government property, as well as exportation and attempted exportation of defense articles without a license. (ECF No. 1.)

Defendant has filed this Motion to Suppress (ECF No. 92) arguing that all information obtained from her military computer, including emails between her and her husband, should be suppressed for violation of the Fourth Amendment. Defendant maintains that anything seized as a result of any ensuing warrants based upon the information in her computer should likewise be suppressed as fruit of the poisonous tree.

II. ANALYSIS

Defendant claims her employer—the Government—violated her Fourth Amendment rights when it searched her computer. A defendant claiming her Fourth Amendment rights were violated by a search must show that she has a "legitimate expectation of privacy in the place searched or the item seized." *United States v. Zeigler*, 474 F.3d 1184, 1189 (9th Cir. 2007). This expectation is shown when the claimant demonstrates both that she had a subjective expectation of privacy in the area searched and that she had an objectively reasonable expectation of privacy in the area. *Id.* It is defendant's burden to prove both of these elements. *Id.*

The Fourth Amendment clearly applies when the Government acts in its capacity as an employer. *City of Ontario v. Quon*, 560 U.S. 746, 756 (2010); *see also O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) ("Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer."). Furthermore, computers can be particularly private spaces worthy of Fourth Amendment protection. *See, e.g., Zeigler*, 474 F.3d at 1189.

However, public employees' expectations of privacy in their offices or computers "may be reduced by virtue of actual office practices and procedures or by legitimate regulation." *O'Connor*, 480 U.S. at 717. "[T]he validity of [any] expectation [of privacy] depends entirely on its context." *Zeigler*, 474 F.3d at 1189.

Although use of a password on the computer can demonstrate a subjective expectation of privacy, *id.*, in this case Defendant signed a User Agreement where she specifically agreed that the security measures being taken—that is, an access card and PIN number to access her computer—were installed to protect the Government's interests, not for her own personal privacy, (ECF No. 92, Exh.1). She received a reminder specifically reiterating this caution every time she used her computer. (ECF No. 95.) Thus, despite the password protection, she could not have had a subjective expectation that the communications from her computer were private.

Furthermore, Defendant received extensive warnings, both at the time her computer was issued and her User Agreement was signed, as well as every time she opened her computer and saw the banner admonishment, that the Government routinely monitored, intercepted, inspected and seized communications made using her computer. She was specifically told that the Government would be looking at her communications for evidence of criminal wrongdoing, personnel misconduct and/or counterintelligence violations. (ECF Nos. 92, Exh.1; 95.) As such, she also had no objectively reasonable expectation that documents and emails on her computer would be private. *See United States v. Greiner*, 235 F. App'x 541, 542 (9th Cir. 2007) ("[P]rivacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the system administrators may monitor communications by the user." (quoting *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007))).

Defendant relies heavily on *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006), to support her argument that she still maintained an expectation of privacy in her computer despite the banner warnings. However, the court in *Long* simply found that the lower court was not clearly erroneous in determining that the defendant had a subjective expectation

of privacy in his military workplace computer emails. The court relied heavily on the testimony of the network administrator who repeatedly said that the agency practice was to recognize the privacy of employees' emails and that the banner described access that would be completed to monitor the computer system and not to examine the contents of the emails. Policies in place limited the network administrator's access to employees' private emails. No such evidence has been presented in this case. *See United States v. Larson*, 66 M.J. 212, 216 (C.A.A.F. 2008) (distinguishing *Long* for the same reasons).

Defendant argues that, despite the User Agreement and the banner warnings, she still had an expectation of privacy in her emails to and from her husband because the User Agreement specifically stated that an employee maintained all other applicable privileges. Since she had a marital communication privilege with respect to her communications with her husband, she argues, she reasonably expected that her employer would not look at these communications.

As an initial matter, the Court takes notice of the fact that, although the Government maintained that it would attempt to honor all other privileges, users needed to take reasonable steps to identify privileged communications as such, so that the Government would not unintentionally peruse privileged documents. Additionally, the Government "strongly encouraged" users to seek personal legal counsel before using the government computers to communicate any privileged material. Defendant took neither of these precautions.

More importantly, however, in order for a marital communication to be privileged, the party must have a reasonable expectation that the communications are confidential. *United States v. Marashi*, 913 F.2d 724, 720 (9th Cir. 1990); *United States v. Hamilton*, 701 F.3d 404, 408–09 (4th Cir. 2012) (affirming determination of no marital privilege when defendant took no steps to protect emails, even after he was on notice of employer's policy permitting inspection of emails at employer's discretion). As discussed above, given the vast array of warnings given to Defendant, she could not reasonably have expected that any communications using her computer would be kept confidential.

Additionally, the marital communication privilege does not apply to communications having to do with joint participation in a criminal endeavor. *Marashi*, 913 F.2d at 731. The communications seized from Defendant's computer reflected her communications with her husband planning the conspiracy with which she is now charged and to which her husband has already pled guilty. Therefore, the communications were not subject to the marital communications privilege. The fact that Defendant may have thought they were privileged may go to her subjective expectation of privacy, but she still fails to show that any expectation was objectively reasonable.

Furthermore, even if Defendant had a reasonable expectation of privacy in this computer, the workplace exception laid out by the plurality in *O'Connor v. Ortega* applies. In *O'Connor*, the Court held that any non-investigatory work-related intrusion by an employer or an investigatory search for evidence of suspected work-related employee misfeasance is inherently reasonable and not a violation of the Fourth Amendment. 480 U.S. at 721–722; *see also Quon*, 560 U.S. at 760 (noting the special needs of the workplace is one area where a search warrant may not be required, as long as search is motivated by a legitimate work-related purpose and was not excessive in scope); *United States v. Slanina*, 283 F.3d 670, 679 (5th Cir. 2002) ("Under *O'Connor*, a search by a government employer must be justified at its inception and reasonably related to the circumstances justifying the interference in the first place."), *vacated on other grounds*, 537 U.S. 802 (2002).

In this case, Defendant had a classified security clearance. An officer from SRT-I expressed concern that Defendant was compiling a list of NSW Command deployment personnel records. Thus, Defendant's employer had a legitimate reason to conduct an investigatory search for evidence of possible work-related misfeasance. The fact that the misfeasance could potentially also be criminal conduct is of no import. *See Slanina*, 283 F.3d at 678 ("*O'Connor*'s goal of ensuring an efficient workplace should not be frustrated simply because the same misconduct that violates a government employer's policy also happens to be illegal."). Nor is it relevant that the government ultimately found no

evidence of misfeasance with respect to the compiling of personnel records but, instead, found evidence of other criminal activity. The search that led to the discovery of the criminal activity was reasonable under the *O'Connor* work place exception.

III. CONCLUSION

For the reasons stated above, Defendant's Motion to Suppress Evidence (ECF No. 92) is **DENIED**.

IT IS SO ORDERED.

DATED: December 7, 2020

Hon. Cynthia Bashant
United States District Judge