Katherine Rohde
Fried, Pierce, & Simon LLP
1375 East 9th Street
Riverside, CA 92501
(951) 906-1000

Attorneys for Jeffrey Popoviz

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION

PRAVEEN PATEL, Plaintiff, v. JEFFREY POPOVIZ, in his individual capacity, Defendant	Case No. 20-cv-0447-JGB

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION FOR SUMMARY JUDGEMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

OTHER AUTHORITIES

INTRODUCTION

Government employers must be allowed to take reasonable steps to protect their workplace from the potential favoritism and harassment that can stem from inappropriate romantic relationships between supervisors and subordinates. As Director of the Office of Personnel Management, Jeffrey Popoviz is entrusted with ensuring the integrity of the California Department of Social Services workplace. Praveen Patel, as Director of the Division of Youth and Family Services, began a romantic relationship with his immediate subordinate in secret and in direct violation of CDSS policy. After receiving a complaint from one of Patel's deputies alleging favoritism and detecting a romantic dinner for two on Patel's travel expense report, Popoviz carried out his duty by implementing a tailored search of Patel's iPad Inbox for evidence of an inappropriate workplace relationship in connection with the dinner. Because Patel failed to create separate inboxes for his work and personal email accounts, the search returned a personal Gmail chain proving the existence of the relationship. Patel was subsequently fired. He later brought this suit, alleging the search violated the Fourth Amendment.

A plaintiff can only prevail on a claim for a Fourth Amendment violation caused by a government workplace search if he can prove that (1) he had a reasonable expectation of privacy in the materials searched and (2) the search was unreasonable under all the circumstances. A reasonable expectation of privacy can be negated by the existence of countervailing workplace policies or practice. Furthermore, the employer has no obligation to implement only the least intrusive search method possible; a search is reasonable if it is justified at its inception and the measures adopted are reasonably related to the objectives of the search without being excessively intrusive. First, Patel had no reasonable expectation of privacy in his iPad Inbox because he was on notice of CDSS practice and policy of reviewing work-related electronic information. Second,

the search was reasonable because it was founded on a reasonable suspicion of wrongdoing and was narrowly tailored to the subject matter at issue. Summary judgement must be granted for the defendant because, as a matter of law, the search was valid under the Fourth Amendment.

STATEMENT OF MATERIAL FACTS

Jeffrey Popoviz has worked for the California Department of Social Services (CDSS) for seven years. (Deposition of the Defendant, Jeffrey Popoviz ("Popoviz Dep."), at 3:14, attached as Ex. A). In his role as Director of Personnel Management, he is entrusted with enforcing CDSS's employment policies to ensure a safe and effective workplace, as well as with final decision-making regarding hiring and firing of Department employees. (Popoviz Dep. 4:11-17). Praveen Patel, the Plaintiff, was one such Department employee, working as Director of Youth and Family Services until he was fired in June 2020. (Deposition of the Plaintiff, Praveen Patel ("Patel Dep."), at 3:1-10, attached as Ex. B). Patel was terminated after a workplace investigation revealed he was engaging in an inappropriate workplace relationship with his direct subordinate. (Popoviz Dep. 16: 11-16).

CDSS explicitly forbids a supervisor from engaging in a romantic relationship with his or her direct subordinate in HR Policy 105, citing the potential for partiality and disruptions to the workplace. (CDSS HR Policy 105: Personal Conduct ("Conduct Policy"), attached as Ex. C). As such, a supervisor who violates this policy can be subject to termination. (Conduct Policy). This past year, Popoviz received instructions from the Director of the California Department of Human Resources to notify senior staff that the Department would be stepping up their efforts to enforce HR Policy 105 and investigating reports of inappropriate relationships. (Popoviz Dep. 11:9-17). Popoviz promptly informed the senior staff, including the plaintiff, Praveen Patel. (Popoviz Dep. 12:1-5).

In March of 2020, Zeinab Ali came to Popoviz's office with an account of workplace impropriety concerning her then supervisor Praveen Patel. (Popoviz Dep. 6:19-22). As Director of Youth and Family Services, Patel supervised three Deputy Directors – Zeinab Ali, Bob Baum, and Anna Wolfe. (Patel Dep. 3:14-4:5). Ali came to Popoviz because she suspected that Patel was engaged in an inappropriate romantic relationship with Deputy Wolfe. (Popoviz Dep. 6:19-22). According to Ali, Patel gave preferential treatment to Wolfe, assigning her high-visibility projects and inviting her to accompany him to work meetings upstate. (Popoviz Dep. 7:16-21). Following their conversation, Popoviz resolved to keep an eye out for evidence of inappropriate behavior from Patel but took no immediate action. (Popoviz Dep. 8:2-3).

However, in June 2020, Popoviz noted a discrepancy in Patel's expense report. (Popoviz Dep. 8:6-7). Earlier that month, Patel and Wolfe, along with the two other Deputy Directors, had attended the Association of Government Social Services Professionals (AGSSP) conference in Santa Barbara. (Popoviz Dep. 8:9-13). Patel had requested to be reimbursed for a dinner for two at Bouchon, a restaurant that Popoviz knew to be "notoriously romantic." (Popoviz Dep. 13-15). Patel had sought reimbursement for $172.77, including a $55 bottle of Heitz Cellar Sauvignon Blanc. (Bouchon Receipt, dated June 1, 2020, attached as Ex. D). Popoviz then recalled Patel and Wolfe had returned one day later than everyone else who attended the conference. (Popoviz Dep. 15-18).

Armed with this evidence and in accordance with his duties as Personnel Director, Popoviz resolved to determine if Patel and Wolfe were in a romantic relationship contrary to CDSS policy and reached out to the IT office for help in the investigation. (Popoviz Dep. 8:20-9:2). The IT department had previously assisted Popoviz in investigating another prior employee, Fred Purcell, for submitting false expense reports. (Popoviz Dep. 9:4-8). IT had been able to

secure Purcell's personal laptop from his office during the workday and search for the original reports. (Popoviz Dep. 9:7-12). According to Popoviz, "everyone in the office knew what was happening." (Popoviz Dep. 9:12). Because enlisting the IT department in his investigation had been an efficient and expedient practice previously, Popoviz asked Jenny Lin, the IT Officer on duty, if she could search Patel's email messages for emails between Patel and Wolfe for evidence of an inappropriate relationship in connection with the Bouchon dinner. (Popoviz Dep. 9:17-20). Lin responded that she could search CDSS servers; the search would take up to a week and would not have access to emails stored locally that were no longer retrievable from the network servers. (Popoviz Dep. 10:5-8, 11:3-4). Alternatively, Lin explained that she could search the email on Patel's iPad, which he had unlocked and dropped off earlier that day for software updates. (Popoviz Dep. 10:1-5). The search would take less than a day. (Popoviz Dep. 11:1-3).

Patel had taken advantage of the Mobile-Computing Device Policy and used his personal iPad for CDSS work. (Patel Dep. 11:5-7); (CDSS Information Technology Policy ("IT Policy") at 1, attached as Ex. E). The Mobile-Computing Device Policy allows employees to conduct CDSS-related business on their personal devices so long as they comply with certain security requirements, such as using an encryption password, and record the device with CDSS's IT unit. (IT Policy at 1). Employees must also grant CDSS's IT access to the device to install software updates as needed. (IT Policy at 2). The device is also subject to the Privacy in the Electronic Environment policy, under which CDSS reserves the right to access and review any work-related electronic information. (IT Policy at 1). CDSS also reserves the right to access employee's email or computer accounts without the employee's consent when there is a reasonable basis to believe that such access may yield information necessary for the investigation of a suspected CDSS policy violation. (IT Policy at 1). When Patel was hired, he signed a form acknowledging that he

had received and read these policies. (Employee Acknowledgement of IT Policies ("IT Acknowledgement"), attached as Ex. F). It is undisputed he agreed to abide by and be bound by these policies. (IT Acknowledgement).

Popoviz instructed Lin to run both searches. (Popoviz Dep. 11:6). He asked her to search Patel's iPad Inbox for emails containing the search terms "Wolfe" or "Anna" and one of the terms "Santa Barbara," "SB," "Bouchon," "dinner," or "AGSSP." (Popoviz Dep. 12:8-11). Popoviz also instructed Lin to restrict the search to April through June 2020. (Popoviz Dep. 12:8-9). He ordered her to not open any data or application on the iPad other than the email Inbox. (Popoviz Dep. 12:14-15). Because Patel had chosen to commingle his iPad Inbox instead of storing his work emails separately, the search would recover messages sent over both Patel's work and personal Gmail account if the message was sent within the allotted timeframe and contained the relevant search terms. (Popoviz Dep. 14:5-12). As such, the search revealed a personal Gmail chain wherein Patel and Wolfe planned their dinner date at Bouchon, confirming Popoviz's suspicion that Patel was in a romantic relationship with his subordinate. (Popoviz Dep. 13:9-17); (Email Chain Gmail RE: Re: AGSSP ("Email Chain"), attached as Ex. G).

Following the search, Popoviz interviewed Wolfe and Patel separately, and both admitted to being romantically involved. (Popoviz Dep. 15:18-22). After consulting his supervisor and confirming that the relationship violated CDSS's Personal Conduct Policy, Popoviz met with Patel and terminated his employment. (Popoviz Dep. 16:2-16). Patel later initiated this action, seeking monetary damages for an alleged violation of the Fourth Amendment. (Compl. at 1:11-13, July 17, 2020, attached as Ex. H).

STANDARD OF REVIEW

Summary judgment must be granted when there is no genuine dispute as to any material facts and the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a). Material facts are facts that might affect the outcome of the suit under the governing law. *Anderson v. Liberty Lobby, Inc.*, 447 U.S. 242, 248 (1986). Although all evidence must be construed in the light most favorable to the nonmoving party, no genuine dispute of material fact is present unless a reasonable jury could return a verdict for the nonmoving party. *Id.* A court must grant summary judgment if the nonmoving party has failed to establish an essential element to its claim. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986); *Khachatourian v. Hacienda La Puente Unified Sch. Dist*., 572 F. App'x 556 (9th Cir. 2014) (affirming grant of summary judgment because public employee's Fourth Amendment rights were not violated by workplace search).

ARGUMENT

I. SUMMMARY JUDGMENT MUST BE GRANTED BECAUSE PATEL HAD NO REASONABLE EXPECTATION OF PRIVACY AND THE SEARCH WAS REASONABLE UNDER ALL THE CIRCUMSTANCES

Summary judgment must be granted because Patel had no reasonable expectation of privacy in his commingled iPad Inbox and the search was reasonable at inception and in scope. Patel has brought suit under 42 U.S.C. § 1983, which provides an individual the right to sue state government employees acting "under color of state law" for violating their constitutional rights. 42 U.S.C.A. § 1983 (Westlaw through Pub. L. No. 116-259). Patel alleges the search of his commingled iPad Inbox violated the Fourth Amendment. (Compl. at 1:11-13). The Fourth Amendment, incorporated against the states by the Fourteenth Amendment, protects individuals against unreasonable searches and seizures by the government, and these protections apply when

the government acts in its capacity as an employer. U.S. Const. amend. IV; U.S. Const. amend XIV; *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 756 (2010).

However, the Supreme Court has held that requiring a public employer to obtain a warrant prior to conducting a workplace search would be "unduly burdensome" and seriously disruptive to the workplace environment. *O'Connor v. Ortega*, 480 U.S. 709, 722 (1987) (plurality opinion). Instead, the test for determining whether a workplace search violates the Fourth Amendment is (1) whether the employee had a reasonable expectation of privacy and (2) whether the search was nevertheless reasonable under all the circumstances. *Id.* at 715, 725-726. The reasonableness of an expectation of privacy is context dependent and can be diminished by the operational realities of the workplace, such as office practices and procedures. *Id.* at 717. Furthermore, a search is only unreasonable if it is unjustified at its inception or if the measures adopted are not reasonably related to the objectives of the search. *Id.* at 726. In assessing the reasonableness of a workplace search, courts must weigh the invasion of the employee's privacy expectation against the government's legitimate need for supervision, control, and efficient operation of the workplace. *Id.* at 719.

Here, Patel could not reasonably expect to maintain privacy in his commingled iPad Inbox because he was on notice of an existing CDSS policy and practice of accessing work-related electronic information. The search of the iPad Inbox was justified at inception because a coworker's allegation of Patel's involvement in an inappropriate workplace relationship, coupled with an abnormal request for reimbursement, created a reasonable suspicion that a search would provide evidence of misconduct. Finally, the search was reasonable in scope because Popoviz took several steps to limit its degree of intrusiveness, restricting the search to the timeframe and subject matter at issue in the investigation.

A. Patel Had No Reasonable Expectation of Privacy in his Commingled iPad Inbox in Light of the Operational Realities of the CDSS Workplace

The court should grant summary judgment because, in light of the broader workplace policy and practice, Patel had no reasonable expectation of privacy. A reasonable expectation of privacy exists where a person has a subjective expectation of privacy and the expectation is one that society is prepared to recognize as reasonable. *United States v. Taketa*, 923 F.2d 665, 676 (9th Cir. 1991) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). Whether an individual has an actual expectation of privacy turns on whether they sought to preserve the item in question as private. *Fazaga v. Fed. Bureau of Investigation*, 965 F.3d 1015, 1034 (9th Cir. 2020) (citing *Bond v. United States*, 529 U.S. 334, 338 (2000)). For the purposes of this motion, the defendant concedes that Patel had a subjective expectation of privacy**.** (Patel Dep. 11:14-20); *United States v. Ziegler*, 474 F.3d 1184, 1189 (9th Cir. 2007) (holding that the use of a password on a computer establishes a subjective expectation of privacy); *Khachatourian v. Hacienda La Puente Unified Sch. Dist.*, No. CV1008436SJORZX, 2012 WL 12877986, at *7 (C.D. Cal. Jan. 24, 2012), *aff'd*, 572 F. App'x 556 (9th Cir. 2014) (explaining that on summary judgment, a court will accept as true the plaintiff's claim that he had a subjective expectation of privacy to avoid making credibility determinations).

However, whether or not an employee's expectation of privacy is reasonable differs according to context and must be determined on a case-by-case basis. *O'Connor*, 480 U.S. at 715, 718. In *O'Connor*, the court held that "the privacy interests of government employees in their place of work… while not insubstantial, are far less than those found at home or in some other contexts." *Id.* at 725. Furthermore, the operational realties of the workplace such as actual office practices and policies may negate the reasonableness of an expectation of privacy. *Id.* at 717. Even an expectation of privacy in one's personal belongings may be unreasonable in light

of a workplace policy or practice. *United States v. Gonzalez*, 300 F.3d 1048, 1055 (9th Cir. 2002). In the context of electronic communications, courts have held an expectation of privacy to be unreasonable when the employee is on notice of their employer's ability to access those communications. *United States v. Greiner*, 235 F. App'x 541, 542 (9th Cir. 2007).

The Supreme Court has previously held that modern personal devices raise unique privacy concerns because of the depth and breadth of private information they can contain. *Riley v. California*, 573 U.S. 373, 393 (2014). However, the court in *Riley* did not establish a per se reasonable expectation of privacy in one's cell phone. *Id.* at 401-402. The court only held that the diminished privacy interests of an arrestee did not justify a warrantless cell phone search, leaving open the possibility that other contexts with reduced privacy expectations (such as the workplace) may justify such a search. *Id.* When dealing with the reasonableness of an expectation of privacy in the context of workplace investigation, the framework laid out in *O'Connor* is more instructive than *Riley*. *Larios v. Lunardi*, 442 F. Supp. 3d 1299, 1308 (E.D. Cal. 2020).

1. CDSS Policies Regarding Access and Review of Work-Related Electronic Information Placed Patel on Notice That He Could Not Reasonably Expect to Maintain Privacy in his Commingled iPad Inbox.

Because Patel was on notice that CDSS had a workplace policy of accessing and reviewing work-related electronic information, including email messages on mobile-computing devices, an expectation of privacy as to his commingled iPad Inbox was objectively unreasonable. Reasonable expectations of privacy on a computing device may be reduced if the user is on notice of a policy that the information is not confidential. *United States v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007). An individual is on notice of a privacy policy if they sign a form acknowledging the policy's existence. *Gonzalez*, 300 F.3d at 1052.

When a workplace policy reserves the right of the employer to access electronic information, an expectation of privacy with respect to that electronic information is objectively unreasonable. *Wasson v. Sonoma Cty. Jr. Coll. Dist.*, 4 F. Supp. 2d 893, 906 (N.D. Cal. 1997). In *Wasson*, an instructor at a junior college alleged that the search and retrieval of documents from her computer during a workplace investigation constituted an unreasonable search and seizure. *Id.* at 901. District policy stated that computer programs and files were confidential unless they had been disclosed by the employee. *Id.* at 906. However, because the computer policy also reserved the right of the district to access all information stored on district computers (with advance notice, if practical) the court held that the instructor could not have had a reasonable expectation of privacy. *Id.*; *see also United States v. Caputo*, No. 3:18-CR-00428-IM, 2019 WL 5788305, at *4 (D. Or. Nov. 6, 2019) (finding any expectation of privacy in email messages objectively unreasonable when computer use policies stated U.S. Government could inspect computer data).

Here, because CDSS reserved the right the access any work-related information, Patel's expectation of privacy in his iPad Inbox was objectively unreasonable. Like in *Wasson*, where the District reserved the right to access all information stored on district computers, here, CDSS policy explicitly reserves the right for CDSS to access "*any* work-related electronic information (data, communications, or *whatever form it takes*)." (IT Policy at 1) (emphasis added). While the policy in *Wasson* was limited to district computers, the CDSS policy is broader, encompassing any work-related electronic activity, including those present on mobile-computing devices. (IT Policy at 1). Furthermore, unlike in *Wasson*, where the policy assures notice will be given if practical, the CDSS policy explicitly disclaims any notice requirement, reserving the right to access an employee's email without the employee's consent when there is reasonable basis to

believe such access may aid in a workplace investigation of a CDSS policy violation. (IT Policy at 1). The computer policy in *Wasson* constitutes a lesser invasion of privacy than the CDSS policy, and the court in *Wasson* nevertheless found an expectation of privacy to be objectively unreasonable. As such, a similar finding that Patel had no reasonable expectation of privacy when on notice of the CDSS policy is required by law.

Furthermore, signing an acknowledgement of a workplace policy may limit the reasonableness of a privacy expectation even in one's personal belongings or communications. *Gonzalez*, 300 F.3d at 1052; *Quon*, 560 U.S. at 762. In *Gonzalez*, a government employee at an Air Force base exchange contested the constitutionality of a random search of his personal backpack. 300 F.3d at 1050. When the employee was hired, he had signed a form acknowledging that the store conducted random checks of personal belongings in order to deter theft by employees and that he might be subject to such searches. *Id.* at 1052. The court found the existence of this policy limited a reasonable expectation of privacy in the backpack, as the employee was on notice that such searches could occur. *Id.* at 1055. Additionally, in *Quon*, the court found it would be unreasonable for a police officer to believe that his personal messages on a department-issued pager were immune from scrutiny, given that the officer had signed a statement acknowledging the existence of a workplace policy allowing the department to audit all communications. 560 U.S. at 762. The court reasoned that the officer knew or should have known his pager messages might be searched during a workplace investigation. *Id.* Because the officer had chosen to commingle his work and personal life by sending personal messages on a work-issued device, those personal messages were subject to workplace policies that limited an expectation of privacy. *Id.*

Even though Patel personally purchased his iPad, he was on notice that the contents of his iPad Inbox were subject to CDSS policies, diminishing any reasonable expectation of privacy. Just as in *Gonzalez*, where the employee signed a form acknowledging a workplace policy of searching personal belongings, here, it is undisputed that Patel signed a form acknowledging and agreeing to abide by the CDSS Information Technology Policies, including CDSS's right to access emails on mobile computing devices. (Patel Dep. 10:1-11); (IT Acknowledgement). Even though Patel did not recall the specific instance of signing the acknowledgement form, his ability to recount the general requirements of the Mobile-Computing Device Policy, as well as his compliance with those regulations (i.e., leaving his iPad with IT for software updates) reflects an awareness of CDSS's IT policies. (Patel Dep. 11:15-20). Furthermore, it was Patel's own choice to commingle his Inbox, thus bringing his personal email messages under CDSS oversight. (Patel Dep. 12:17-19). As in *Quon*, Patel knew or should have known that the emails in his iPad Inbox could be subject to a valid workplace search. (IT Policy at 1). As such, his decision to commingle his personal and work emails in that Inbox could not have been made with an expectation of privacy that was reasonable.

Expectations of privacy are further diminished when an employee is on notice via a workplace policy that the employer will search their electronic communications for evidence of specific wrongdoing. *United States v. Ye Sang Wang*, No. 19-CR-1895-BAS, 2020 WL 7226442, at *3 (S.D. Cal. Dec. 8, 2020). In *Ye Sang Wang*, a logistics specialist for the Department of Defense challenged the search of her email communications which revealed evidence of a plan to sell military items overseas. *Id.* at *2. The court held that the employee had no reasonable expectation of privacy because the Department computer policy stated that communications could be searched for evidence of criminal wrongdoing, personnel misconduct, or

counterintelligence violations. *Id.* at *3. Similarly, the CDSS privacy policy states that employees' emails may be searched without their consent when there are reasonable grounds to believe the search may reveal evidence of illegal conduct or a CDSS policy violation. (IT Policy at 1). Patel was also personally informed at an April staff meeting that CDSS would be stepping up its efforts to enforce their policy prohibiting intradepartmental relationships. (Popoviz Dep. 11:18-12:3). At this point, Patel had already been in a romantic relationship with his direct subordinate for two months. (Patel Dep. 5:17-19). He knew he was violating CDSS policy. (Popoviz Dep. 11:18-12:3). He knew evidence of that violation was present in his iPad Inbox. (Email Chain). He knew that CDSS had the right to access his emails to investigate policy violations and that they would be investigating allegations of intradepartmental relationships. (IT Policy at 1). Any expectation of privacy as to the emails on his iPad under these circumstances was objectively unreasonable.

2. Previous CDSS Practice of Searching a Mobile Computing Device During Misconduct Investigations Belies Reasonableness of Patel's Expectation of Privacy in His Own Mobile Computing Device.

Patel's expectation of privacy in his commingled iPad Inbox was also objectively unreasonable in light of previous workplace searches of mobile computing devices. Expectations of privacy are unreasonable when an employee is on notice that searches of the type to which he was subjected might occur for work-related purposes. *Khachatourian*, 2012 WL 12877986, at *8. In *Khachatourian*, a public high school teacher challenged the constitutionality of a search of his classroom by trained dogs. *Id.* at *4. However, the court held that the teacher did not have a reasonable expectation of privacy since he was on notice that searches of this type could and would occur, relying on the teacher's own account that dogs had searched his room on previous occasions. *Id.* at *8 (citing *Schowengerdt v. Gen. Dynamics Corp.*, 823 F.2d 1328 (9th Cir.

1987)). The court found that knowledge that the District had a practice of such searches made an expectation of privacy unreasonable. *Id.*; *see also Shaffer v. Field*, 339 F. Supp. 997, 1003 (C.D. Cal. 1972) (finding no reasonable expectation of privacy in a locker when lockers had been searched by employer on three previous occasions), *aff'd*, 484 F.2d 1196 (9th Cir. 1973).

Because Patel was aware of a CDSS practice of searching mobile computing devices for evidence of employee misconduct, it would similarly be unreasonable to expect privacy in his own mobile computing device. Like in *Khachatourian*, where the teacher was aware of prior dog searches, here, Patel was aware that IT had confiscated and searched an employee's laptop just six months prior in service of a workplace investigation. (Patel Dep. 16:1-3). Although Patel assumed the device confiscated was not a personal laptop, he was nevertheless aware that a mobile computing device of similar function to his own, similarly equipped with CDSS programs and email services, was confiscated to investigate a violation of CDSS policy. (Patel Dep. 15:11-16:6). An expectation of privacy was unreasonable in light of workplace practice.

B. The Search of Patel's Commingled iPad Inbox was Reasonable Under All the Circumstances Because It Was Justified at Inception and Narrow in Scope

Regardless of whether Patel had a reasonable expectation of privacy in his commingled iPad Inbox, the court should nevertheless grant summary judgment because the search was reasonable under all the circumstances. A workplace search is only unreasonable if it is unjustified at its inception or impermissible in scope. *O'Connor*, 480 U.S. at 726. A search is justified at inception when there are reasonable grounds for suspecting that the search will provide evidence of employee work-related misconduct. *Id.* Furthermore, a search is permissible in scope when the chosen method is "reasonably related to the objectives of the search and not excessively intrusive" in light of the nature of the suspected misconduct. *Id.* (citing *New Jersey v. T.L.O.*, 469 U.S. 325 (1985)). In making these determinations, the court must balance the

invasion of the employee's privacy interest against the public employer's need for "supervision, control, and efficient operation of the workplace." *Id.* at 719-720. Here, the search was justified at inception because Popoviz had reasonable suspicion a search would reveal evidence of employee misconduct. The search was reasonable in scope because Popoviz limited the timeframe of emails reviewed and implemented a tailored search algorithm to only return messages relating to the dinner between Patel and Wolfe at the AGSSP conference.

1. The Search was Justified at Inception Because Popoviz had a Reasonable Basis to Believe a Search Would Reveal Evidence of an Inappropriate Workplace Relationship Between Patel and Wolfe.

Patel's coworker's allegation that he was involved in an inappropriate workplace relationship, coupled with the abnormal expense report, created a sufficient basis for the commencement of a workplace investigation. When a search is implemented following a coworker's general allegation of office misconduct, the search is justified at inception. *Taketa*, 923 F.2d at 674. In *Taketa*, a Drug Enforcement Administration (DEA) agent was using agency resources to impermissibly engage in wiretapping activity. *Id.* at 668. The supervisor first become aware of potential employee misconduct when a fellow employee reported her suspicions that the agent had modified a DEA pen register to intercept telephone conversations. *Id.* The supervisor subsequently initiated an investigation. *Id.* The court held that the fellow agent's general allegation provided a sufficient basis for the commencement of an internal investigation. *Id.* at 674.

In this case, Popoviz similarly received a report from a coworker alleging wrongdoing; Deputy Director Zeinab Ali reported that Patel was violating HR Policy 105 by engaging in a romantic relationship with his direct subordinate. (Popoviz Dep. 6:19-22). Arguably, under the rule in *Taketa*, Popoviz would have been justified in carrying out an investigation even after this

general allegation. Popoviz instead exercised caution, keeping an eye out for evidence of specific misconduct. (Popoviz Dep. 8:1-3). Such evidence arrived three months later in the form of an expense report requesting reimbursement for a romantic dinner for two during a work trip. (Popoviz Dep. 8:9-18). Now that Popoviz had become aware of a specific instance that, if properly investigated, would reveal concrete evidence of an inappropriate workplace relationship, he carried out his duty in investigating the issue. (Popoviz Dep. 8:20-9:2). Between Ali's allegation and the abnormal expense report, Popoviz had reasonable grounds to suspect that an investigation would provide evidence of workplace misconduct.

2. The Search of Patel's Commingled iPad Inbox was Reasonable in Scope Because Popoviz Implemented a Search Algorithm Narrowly Tailored to the Time and Subject Matter Related to the Misconduct

The search was reasonable in scope because it was limited to messages that met a highly specific search algorithm within a narrow three-month window. A search is permissible in scope when the chosen methods are reasonably related to the aim of the search while refraining from becoming overly intrusive of the employee's legitimate privacy interests. *O'Connor*, 480 U.S. at 726. The scope of a search is not too intrusive when an employer takes steps to tailor the inquiry to the materials and timeframe at issue. *Quon*, 560 U.S. at 761-762. Reading an employee's communications, even if personal or on a privately owned device, can remain permissible in scope when employers take such tailoring steps. *Id.* Additionally, employers are not required to adopt the least intrusive method available; it is enough that they elect an efficient and practicable approach. *Id.* at 763.

When determining whether a search was too intrusive, courts balance the employee's expectation of privacy against the government's need for supervision and the severity of the alleged misconduct. *O'Connor*, 480 U.S. at 719-720. The extent of an employee's reasonable

expectation of privacy is relevant; if an employee has only a limited expectation of privacy in the materials at issue, then a search will not be overly intrusive. *Quon*, 560 U.S. at 762. As previously discussed, Patel's expectation of privacy in his iPad Inbox was reduced because he was on notice of CDSS's policy and practice of reviewing work-related electronic information. Furthermore, CDSS had a significant interest in protecting the workplace from the partiality and abuse of power that can arise from a romantic relationship between a supervisor and a subordinate. (Conduct Policy).

When an employer implements a narrow search of electronic communications by redacting irrelevant information and restricting the search to the appropriate timeframe, the search is not too intrusive. *Larios*, 442 F. Supp. 3d at 1310; *Quon*, 560 U.S. at 761-762. In *Larios*, the California Highway Patrol (CHP) began an investigation into one of its officers after evidence appeared that the officer was romantically involved with a CHP confidential informant. 442 F. Supp. 3d at 1303. The court found the investigator's ensuing search of the officer's personal cell phone to be reasonable in scope because they only searched the officer's communications with the informant and limited their search to the months in which the informant worked with CHP. *Id.* at 1310. As such, the investigators took sufficient steps to protect the privacy interests of the officer in light of the serious abuse of power suspected and the important government interest at stake. *Id.*; *see also Quon*, 560 U.S. at 761-762 (finding that a search of an officer's department-issued pager which contained personal messages was not excessively intrusive when it was limited to just two months and off duty messages were redacted).

In the present case, Popoviz implemented a tailored search of Patel's commingled iPad Inbox, restricted in time and subject matter, so the search was not overly intrusive. In *Larios*, the

search was limited to the timeframe in which the officer and informant could have been engaged in an inappropriate romantic relationship – from the month the informant initially contacted CHP with information about a narcotics dealer, to the day before the phone was searched. 442 F. Supp. 3d at 1310. Here, Popoviz limited the search even more narrowly, looking only at emails from April 2020 – a month after Popoviz first became aware of a potential inappropriate workplace relationship – to June 2020 – the month of the "notoriously romantic" dinner that Patel sought to have reimbursed. (Popoviz Dep. 12:8-9). Arguably, Popoviz would have been justified in searching as far back as December 2019, when Wolfe was first hired by CDSS, as this would encapsulate the timeframe in which Patel and Wolfe could have had an inappropriate workplace relationship. (Popoviz Dep. 8:8-12); *see also Quon*, 560 U.S. at 761-762 (holding that while it may have been reasonable for the department to search all the months in which potential misconduct took place, it was certainly reasonable for the department to search just two months of messages). By limiting the search to just three months, Popoviz took care to protect Patel's privacy interests while carrying out his duty to investigate a serious violation of CDSS policy.

Popoviz further tailored the search by implementing narrow search terms designed to capture only information related to the dinner at Bouchon. While the investigators in *Larios* only limited the subject matter of their search by looking at communications between the officer and informant, Popoviz went even further. He designed a search algorithm that would only return conversations containing either "Wolfe" or "Anna" and one of the following key terms: "Santa Barbara," "SB," "Bouchon," "dinner," or "AGSSP," tailoring the search to the romantic dinner-for-two that prompted the investigation. (Popoviz Dep. 12:10-11). Such limited search terms are analogous to redacting irrelevant information, as the investigators in *Quon* did when they redacted off-duty messages, because both approaches restrict the ultimate search results to the

subject matter at issue. While Popoviz's search algorithm captured both work and personal emails, this result was unavoidable given Patel's failure to create separate inboxes. (Popoviz Dep. 14:5-12). In *Quon*, the court held that a search which captured both personal and work messages was permissible in scope because the officer had chosen to comingle his private and professional communications on one device. Furthermore, Popoviz instructed the IT officer to only search the iPad email inbox; no other data or applications were opened. (Popoviz Dep. 12:14-15). Private information identified by the court in *Riley* such as internet browsing history or GPS information were not implicated in this search. 573 U.S. at 394.

Finally, government employers are not required to use a slower or less accurate method in service of achieving the least intrusive search practicable. *Quon*, 560 U.S. at 763. In *Quon*, the Ninth Circuit originally held that the search of an officer's text messages on a work-related device was unreasonable in scope because there were less intrusive alternatives; the court suggested the department could have given the officer advance warning that next month's messages would be reviewed, asked the officer to redact personal messages himself, or requested the officer's permission to conduct the search. *Id.* On review, the Supreme Court criticized this approach, explaining that "judges engaged in *post hoc* evaluations of government conduct can almost always imagine" a less intrusive method. *Id.* Decisions based on such reasoning would seriously undermine the ability of the government to conduct any search or seizure and would represent an overreach of judicial review. *Id.* The court ultimately reversed, concluding that the search of the officer's messages without his permission was reasonable because it was an efficient and expedient method to achieve the objectives of the search. *Id.* at 761.

Here, Popoviz was not required to implement the least intrusive search possible in his investigation of Patel's inappropriate workplace relationship. While it is true that Popoviz could

have chosen to search only the network servers or asked Patel to turn over any incriminating communications of his inappropriate relationship with Wolfe, the existence of such alternatives does not indicate the search as conducted was unreasonable. (Popoviz Dep. 10:5-8). Furthermore, just as in *Quon*, where the alternatives suggested by the Ninth Circuit would have taken longer or been less reliable, here, potential alternatives likely would not have met the objective of the search. Searching the network servers would have taken multiple days and would have failed to capture locally stored emails. (Popoviz Dep. 10:5-8, 11:1-4). Asking Patel to voluntarily incriminate himself would almost certainly not be successful. Popoviz elected a method that was efficient and practical in light of the objectives of the search, while implementing safeguards to protect Patel's privacy interests. An argument that the search was unreasonable based on the premise that less intrusive means were available is inconsistent with controlling precedent.

CONCLUSION

For the foregoing reasons, summary judgment must be granted for the defendant because, as a matter of law, the search of Patel's iPad Inbox did not violate the Fourth Amendment. In light of a legitimate policies and practice granting CDSS access to employee's work-related electronic information, no reasonable jury could conclude that Patel had a reasonable expectation of privacy in his commingled Inbox. After receiving an allegation of inappropriate behavior from Patel's coworker and noting an alarming irregularity in his expense report, Popoviz was justified in initiating the search. The search conducted was narrowly restricted to the timeframe and subject matter related to the alleged misconduct so as to limit any invasion of privacy. As there is no dispute as to any material fact, it follows that summary judgment must be granted for the defendant.

DATED: February 26, 2021

Respectfully Submitted,
Fried, Pierce, & Simon LLP

/s/ Katherine Rohde

Katherine Rohde
1375 East 9th Street
Riverside, CA 92501
(951) 906-1000

ATTORNEYS FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Memorandum of Law in Support of Defendant's Motion for Summary Judgement was served this day via email to counsel for Plaintiff at the following address:

Jeremy Bruckner
Duncan, Gowen, & Firoz LLP
501 Market Street
Riverside, CA 92501
Tel.: (951) 555-5000
Email: jbruckner@dgandf.com
Attorneys for Plaintiff

/s/ Student #1
Dated: February 26, 2021