Lia Rocchino
LINDELL, DUNCAN & DIAZ LLP
501 Market Street
Riverside, CA 92501
Attorney for Nathan Aspinall

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

NATHAN ASPINALL, Plaintiff, v. ELLIS CARTER, in his individual capacity, Defendant.	**No. 23-cv-0447-JGB** **Civil Action**

MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CONSTITUTIONAL PROVISIONS

CASES

RULES

INTRODUCTION

Government employers cannot be permitted to infringe on their employees' digital privacy in response to rumors and hunches alone. In an era where the average cell phone holds the entirety of a person's private life, the bar for privacy must be set higher. Nathan Aspinall, who led a team at the California Department of Social Services ("CDSS"), was one such government employee. As authorized by his workplace's policies, he occasionally used his personal iPad for work purposes, and in compliance with cybersecurity policies, he routinely granted the IT Department access to his device to install software updates. During one such occasion, the Director of Personnel Management instructed the IT Department to take advantage of their access to Aspinall's personal device and run a search of his work and personal email accounts for evidence of an alleged unauthorized intradepartmental relationship. The Director's only reason for suspicion at the inception of this search was a rumor reported several months prior and an expense report line item from a recent government conference. Based on emails obtained in this search, Aspinall was fired from his role at CDSS. He brought this suit alleging that the search violated his Fourth Amendment right against unwarranted search and seizures.

To succeed on their motion for summary judgment, the defendant must first prove that Aspinall's constitutional rights were not implicated because he did not have a legitimate privacy expectation in his personal iPad that society is prepared to recognize as reasonable. A reasonable jury could find that Aspinall did, however, have a reasonable expectation of privacy in his personal device and email because he purchased the device himself, kept it password protected, and CDSS' workplace policies did not put him sufficiently on notice of potential searches to diminish his expectation. Next, if Aspinall is found to have a legitimate privacy expectation in his iPad, the defendant must prove his intrusion for an investigation of alleged workplace

misconduct was reasonable both at its inception and in its scope. A reasonable jury could find Carter's search was unreasonable because it was instigated based on an unparticularized suspicion of misconduct after Carter made a logical leap between a month-old rumor and an expense report line item. In addition, a reasonable jury could find Carter's search of Aspinall's personal emails to be unreasonable in its scope because it was excessively intrusive when balanced against the novel privacy interests at stake and the non-urgent nature of Aspinall's alleged misconduct. Because the balancing test required is a fact-intensive inquiry that implicates unique and novel interests of digital privacy, this case is unsuited for summary judgment and the defendant's motion must be denied.

STATEMENT OF DISPUTED MATERIAL FACTS

Nathan Aspinall is a public servant who led the Division of Youth and Family Services at the California Department of Social Services ("CDSS") in Riverside, CA for two and a half years. (Aspinall Dep. (Oct. 26, 2023), 6:3-6). In this role, he managed a team of over twenty government employees responsible for overseeing the state's child welfare program. (Aspinall Dep. 3:7-13). On June 8, 2023, having recently returned from an annual industry conference in Santa Barbara, Aspinall worked from the office as usual. (Carter Dep. (Nov. 9, 2023), 10:9-13). At some point, he made a pitstop at IT to drop off his personal iPad for routine software updates, unlocking it for IT's ease as he had done many times before. (Aspinall Dep. 14:8-16). By all outward indications, June 8 seemed to Nathan Aspinall to be an entirely typical day.

In fact, earlier that day, without his knowledge or consent, CDSS Office of Personnel Management Director Ellis Carter had, based on a rumor and a hunch, knowingly commissioned an intrusive search of Aspinall's email account – his personal Gmail account, on his personal iPad, with the aim of uncovering information about his personal life. (Carter Dep. 14:16-15:3). A

few weeks later, Nathan Aspinall was fired based on that search. (Carter Dep. 16:11-18).

Aspinall began working at CDSS in January 2021. (Aspinall Dep. 6:6). As with most companies, CDSS onboarded its new hires with a deluge of documents and trainings about the department's policies and technology requirements. (Aspinall Dep. 6:7-15). And like most new employees, Aspinall signed all the requisite documents – like the Mobile-Computing Device policy that permitted employees to use password-protected personal devices for work, like Policy 105 on Personal Conduct that prohibited romantic relationships with subordinates, and like CDSS' Privacy in the Electronic Environment policy. (CA Department of Social Services HR Policy 105: Personal Conduct ("Policy 105"), attached as Ex. 1; CA Department of Social Services Policy 2: Mobile-Computing Device Policy ("Policy 2"), attached as Ex. 3; CA Department of Social Services Policy 1: Privacy in the Electronic Environment ("Policy 1"), attached as Ex. 3; Nathan Aspinall's Acknowledgement and Receipt of Human Resources Policies ("HR Acknowledgement"), attached as Ex. 2; Nathan Aspinall's Acknowledgement and Receipt of Information Technology Policies ("IT Acknowledgement"), attached as Ex. 4). The Privacy in the Electronic Environment policy granted CDSS the right to access "work-related electronic information" without an employee's consent in a limited number of circumstances like emergency situations and to assist in criminal or CDSS policy violation investigations. (Policy 1). Apart from this onboarding, Aspinall was never again told of CDSS' Privacy in the Electronic Environment policy. (Aspinall Dep. 9:10-13). In fact, over two years into Aspinall's employment, he did not recall the policy's content. (Aspinall Dep. 9:10-13).

In Spring 2021, Amy Johnson, a woman with whom Aspinall had worked previously in the private sector, was hired for a deputy role on Aspinall's team. (Aspinall Dep. 4:9-18). After nearly two years of working together, Aspinall and Johnson began dating in February 2023 and

later became engaged. (Aspinall Dep. 5:15-6:2). They decided to keep their romantic relationship separate from their professional lives. (Carter Dep. 7:4-7, 16:20-22).

As Johnson excelled in her role as deputy, her responsibilities and leadership opportunities expanded. (Aspinall Dep. 16:10-20). In March 2023, a CDSS employee told Carter she suspected Johnson and Aspinall were in a relationship because they had been seen eating lunches together and expressed concern that Johnson received special treatment as a result. (Carter Dep. 6:19-7:6). Carter, whose primary role at CDSS was to investigate allegations of misconduct, took no action on this coworker's suspicions for three months. (Carter Dep. 4:13-17, 8:1-7). He did not speak with Aspinall about the rumors until after the iPad search was completed. (Carter Dep. 11:18-12:5).

In June 2023, Aspinall and his three deputies traveled to Santa Barbara for the annual Association of Government Social Services Professionals (AGSSP) conference. (Aspinall Dep. 17:1-7). At the conclusion of the trip, Aspinall submitted his expense report for reimbursement of his hotel and meals during the conference – including team dinners and a dinner with a guest on the final night of the conference. (Aspinall Dep. 17:17-20; Aspinall AGSSP Expense Report (June 5, 2023), ("Expense Report"), attached as Ex. 6). When Carter read Aspinall's expense report on June 8, he assumed immediately that Johnson was Aspinall's dinner guest. (Carter Dep. 8:5-18). His first action upon reading the report was to call CDSS IT Officer Jenny Peng to request a search of Aspinall's email account for evidence of his relationship with Johnson. (Carter Dep. 8:20-9:2). Carter made no attempt to speak with Aspinall about his hunch prior to requesting that IT invade Aspinall's privacy in this way. (Carter Dep. 10:14-18).

Peng told Carter that she could search CDSS' servers for Aspinall's work emails, but that it would take a few days to a week to complete. (Carter Dep. 11:1-4). In addition, she told Carter

that "as luck would have it" Aspinall had dropped off his iPad with IT for software updates, and she would be able to search emails stored on the iPad locally. (Carter Dep. 10:1-8). Peng also informed Carter that due to the nature of how Aspinall had set up his iPad inbox, emails from his personal Gmail account would be uncovered in her search. (Carter Dep. 14:5-18). Carter "wasn't concerned" about the comingling and, with full knowledge that he would be searching through Aspinall's personal email account, initiated the search. (Carter Dep. 14:16-19).

This was not Carter's first time requesting IT to search an employee's personal device. (Carter Dep. 9:3-7). He had initiated a similar search on an employee's personal computer six months earlier to find evidence of alleged falsified expense reports. (Carter Dep. 9:4-10). In that case, IT removed the employee's personal laptop from his office in the middle of the workday. (Carter Dep. 9:10-15). Aspinall, though aware of this incident, was not aware that the confiscated laptop was the employee's personal property. (Aspinall Dep. 16:1-6).

Though Aspinall connected his iPad to the CDSS network and used it for work on business trips and after hours, he purchased it himself prior to joining CDSS and used it primarily as a personal device. (Aspinall Dep. 11:4-12:6). Aspinall kept the device password protected and described the idea that his colleagues could search it without his consent as "unconscionable" and an "abuse" of his trust, saying his "personal life [was] none of their business." (Aspinall Dep. 14:8-15:10). Despite the iPad email app's comingling his two email accounts, Aspinall never sent personal emails from his CDSS email and never intentionally sent work emails from his personal account. (Aspinall Dep. 13:1-10). Johnson occasionally also used the iPad for her work when IT was working on her desktop. (Aspinall Dep. 13:11-17).

Carter ordered a search of all of Aspinall's emails from April through June 2023 with the broad search terms of "Johnson" and "Amy" in the same email as "Santa Barbara," "SB,"

"Bouchon," "dinner," or "AGSSP." (Carter Dep. 12:8-11). The search returned several emails from Aspinall's personal Gmail account between him and Johnson. (Carter Dep. 13:9-19). The emails discussed their trip to AGSSP and, according to Carter, indicated that the two were in a romantic relationship. (Carter Dep. 13:9-19). However, the search did not uncover any emails of a personal nature between Aspinall and Johnson from their CDSS email accounts. (Carter Dep. 13:18-14:1). Only after Carter conducted this search did he schedule individual meetings to ask Aspinall and Johnson about their relationship. (Carter Dep. 15:18-20). Both were forthright about the relationship but clear that they were strictly professional at work and intended to keep their private lives private. (Carter Dep. 15:20-22). Aspinall also denied giving Johnson any preferential treatment as a result of the relationship. (Carter Dep. 15:22-16:2).

After this investigation, Carter and his superior at the state Department of Human Resources together decided that Aspinall had violated CDSS' Personal Conduct Policy. (Carter Dep. 16:2-8). Aspinall was fired effective immediately. (Carter Dep. 16:11-16). As of October 2023, Aspinall has been unable to find employment. (Aspinall Dep. 2:19-3:3). Aspinall initiated this lawsuit, seeking monetary damages for Carter's violation of his Fourth Amendment rights. (Compl. at ¶ 32).

SUMMARY JUDGMENT STANDARD

A motion for summary judgment must be denied unless the moving party shows there is no genuine dispute as to the material facts of the case. Fed. R. Civ. P. 56(a). Material facts are those which are essential under the governing law and thus may affect the outcome of the lawsuit. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986). The moving party bears the initial burden of production and must establish that there is no genuine dispute in order to be entitled to judgment as a matter of law. Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986). A

dispute is genuine when the evidence, with all inferences drawn in favor of the nonmoving party, is such that a reasonable jury could find in favor of that party. Anderson, 477 U.S. at 242. Unless the evidence shows that the dispute is "so one-sided that one party must prevail as a matter of law," the court must deny the motion for summary judgement. Id. at 252.

ARGUMENT

Summary judgment must be denied because a reasonable jury could find that CDSS violated Aspinall's reasonable expectation of privacy by initiating an intrusive warrantless search of his personal iPad and email communications based on a mere hunch of improper conduct. The Fourth Amendment guarantees individuals security "in their persons, houses, papers, and effects against unreasonable searches and seizures." U.S. Const. amend. IV. Under its protection, warrantless searches by government officials are per se unreasonable. City of Ontario, Cal. v. Quon, 560 U.S. 746, 756 (2010). This protection applies equally when the government acts in its capacity as employer. O'Connor v. Ortega, 480 U.S. 709, 717 (1987). In limited cases, the Fourth Amendment's default warrant requirement can be forgone when government employers have a special need to investigate work-related misconduct. Id. at 725. To determine when a search of this kind implicates a government employee's Fourth Amendment rights and thus requires a warrant, the court undertakes a two-step analysis based on a standard of reasonableness. Quon, 560 U.S. at 756. First, a court must assess the employee's reasonable expectation of privacy in light of the operational realities of the workplace. O'Connor, 480 U.S. at 717. Second, the court determines if an employer's intrusion on that legitimate expectation of privacy for work-related or investigatory purposes is unreasonable. Quon, 560 U.S. at 757.

Here, summary judgment must be denied because a reasonable jury could find that Carter's actions constituted an unconstitutional search that impeded on Aspinall's privacy

interest in his personal electronic device. First, Aspinall had a constitutionally cognizable privacy interest in his iPad and email account because his subjective view in the privacy of a device he purchased himself and kept password protected is one society recognizes as objectively reasonable. This view was undiminished by CDSS' electronic privacy policy because it was communicated to employees only during their onboarding process and authorized CDSS to access only work-related materials under limited circumstances. Second, Carter's decision to search Aspinall's comingled email account on his personal iPad was an unreasonable search because it was based on a non-obvious logical leap between a months-old rumor and an expense report. In addition, Carter's search of Aspinall's personal emails was disproportionately intrusive in comparison to the benign nature of the consensual workplace relationship he was investigating.

I. Summary Judgment Must Be Denied Because a Reasonable Jury Could Find that Aspinall's Reasonable Expectation in the Privacy of His iPad Was Not Sufficiently Diminished by CDSS' Limited Workplace Search Policies

A reasonable jury could find that Aspinall's expectation of privacy in his iPad was reasonable because it was a device he purchased himself and kept password protected, and CDSS' policy on electronic privacy did not give him sufficient notice that his device could be subject to searches. When a government employee has an expectation of privacy in an item, his constitutional rights may be implicated by a search of that item. United States v. Ziegler, 474 F.3d 1184, 1189 (9th Cir. 2007). Not all personal items brought into a workplace context fall under the scope of the workplace exception to the Fourth Amendment's warrant requirement; the exception covers only items "related to work" and "within the employer's control." O'Connor, 480 U.S. at 715. Some courts have held that, because personal cell phones are so pervasive an aspect of modern life, an employee's use of a personal device on an employer's premises or

occasionally for work purposes is insufficient to render the device part of the workplace context. Turiano v. City of Phoenix, 562 F.Supp.3d 261, 276 (D. Ariz. 2022) (finding the workplace exception inapplicable to an employee's purely personal cell phone). See, e.g., Riley v. California, 573 U.S. 373, 395 (2014) (stating that personal cell phones are a pervasive aspect of modern society); O'Connor, 480 U.S. at 715-716 (holding the workplace exception does not necessarily apply to a personal item that happens to be within an employer's business address).

An employee's expectation of privacy generally is legitimate when a person exhibits an actual subjective expectation of privacy in the searched item and the expectation is one that society recognizes as reasonable. Ziegler, 474 F.3d at 1189. Because the operational realities of a workplace could make an employee's expectation of privacy unreasonable, the first inquiry is fact-intensive and must be decided on a case-by-case basis. Turiano, 562 F.Supp.3d at 273.

Here, Aspinall believed his iPad to be private both because it was a device he had purchased for his own personal use and because it was password protected. The operational realities of CDSS as a workplace did not sufficiently diminish Aspinall's expectation of privacy because its electronic privacy policy authorized monitoring of limited work-related information and was only communicated to employees once during the onboarding process. A jury could find Aspinall's expectation of privacy was reasonable, and thus summary judgment must be denied.

A. Aspinall Expected His iPad to Remain Private Because It Was a Password-Protected Device He Purchased for Personal Use Prior to Starting at CDSS.

Aspinall had a subjective belief that his iPad was private because it was his personal property that he kept password protected. Personal electronic devices like cell phones and tablets are so pervasive in modern society that many consider them to be essential means of self-expression. Quon, 560 U.S. at 760. Individuals have a strong privacy interest in their electronic devices because such devices contain vast quantities of personal information. Riley, 573 U.S. at

393. As the Supreme Court has acknowledged, "the sum of an individual's private life can be reconstructed" through the data found on a cell phone. Id. at 394.

No one factor determines if an individual has a legitimate subjective belief of privacy. United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007). Individuals have a subjective expectation of privacy in electronic devices they purchase themselves for personal use. Id.; see also Espinoza v. City of Tracy, No. CV 15-751 WBS KJN, 2018 WL 2318335, at *6 (E.D. Cal. May 22, 2018) (finding that a government employee did not have a subjective expectation of privacy in an employer-issued cell phone because it was not his personal property). An individual has a subjective expectation of privacy in an item when there is sufficient evidence they sought to preserve that item as private. Katz v. United States, 389 U.S. 347, 351 (1967). The use of a password on an electronic device is sufficient evidence that an individual had an expectation of privacy in that device. Ziegler, 474 F.3d at 1189.

Here, Aspinall viewed his iPad as his personal and private device. Unlike the employee in Espinoza who used a city-issued cell phone at work, Aspinall purchased his iPad himself before he began working at CDSS. (Aspinall Dep. 11:4-12:6). And as was the case in Ziegler, he kept the device password protected, unlocking it only to allow the IT Department to install required updates. (Aspinall Dep. 14:8-15:10). Though he connected it to his work servers and used it for work occasionally after hours or on business trips, Aspinall viewed the iPad as his personal device. (Aspinall Dep. 11:4-12:6). He called the idea that his coworkers could search his iPad without his permission "unconscionable," saying that his "personal life [was] none of their business." (Aspinall Dep. 14:8-15:10). Akin to the Riley court's expression of the novel privacy concerns implicated by personal devices like cell phones, Aspinall viewed his iPad as a device containing the sum of his private life – including his personal emails – to which he did not

believe his employer should have unwarranted access. (Aspinall Dep. 14:8-15:10).

B. Aspinall's Expectation of Privacy Was Not Diminished by the Operational Realities of the Workplace Because CDSS' Policy Permitted Only Limited Access to Work-Related Materials and Was Not Regularly and Consistently Reaffirmed to Employees.

The workplace realities at CDSS did not defeat the reasonableness of Aspinall's expectation of privacy because the Privacy in the Electronic Environment policy was only communicated to employees during the onboarding process and limited its authorization of searches to work-related materials. When an employee's expectation of privacy is an objectively reasonable one that society is prepared to acknowledge, it triggers Fourth Amendment protections. Katz, 389 U.S. at 361. The actual office practices and communicated procedures shape the reasonableness of privacy expectations. O'Connor, 480 U.S. at 717–18.

A policy authorizing monitoring of devices under limited circumstances does not put employees on sufficient notice that they could be subject to searches. Heckenkamp, 482 F.3d at 1146. In Heckenkamp, the court analyzed if a student's expectation of privacy on his personal computer was destroyed when he attached it to a public university's network. Id. Though the defendant was not an employee, the court applied the same reasonableness standard as is utilized in the workplace context. Id. The university in Heckenkamp did not have a clearly announced monitoring policy in place. Id. at 1147. Their general computing policy, however, stated that personal computer files saved on the network would be free from access from unauthorized users except in limited cases to protect the university's systems or the rights and property of the state. Id. The court held that the policy established only limited circumstances in which administrators could access the student's computer and therefore did not defeat the objective reasonability of the student's expectation of privacy. Id.

Here, CDSS' electronic privacy policy did not give Aspinall sufficient notice that his

personal iPad and email could be searched because it authorized monitoring of only work-related information and under limited circumstances. Aspinall connected his personal device to a government-owned network just as did the student in Heckenkamp. (Aspinall Dep. 11:4-12:6). And similar to the policy in Heckenkamp that stated private devices would be in general free from monitoring, CDSS' policy explicitly authorized the department to monitor only "work-related electronic information," but not personal devices or personal information. (Policy 1). Similar to the lack of clarity in Heckenkamp on an established monitoring policy, CDSS' policy language did not clearly authorize them to access work-related information on personal devices used in the workplace. (Policy 1). And like the policy in Heckenkamp that put students on notice that under limited circumstances their computers could be monitored, CDSS' policy set out limited circumstances under which it could access employee's work-related information. (Policy 1). Though the policy authorized access to investigate CDSS policy violations, a reasonable jury could conclude that this limited authorization is insufficient to override an employee's general objective expectation of privacy in a device as full of personal information as an iPad.

A singular notification that a workplace's electronic information is subject to monitoring is insufficient to defeat an employee's expectation of privacy. United States v. Caputo, No. 3:18-CR-00428-IM, 2019 WL 5788305, at *4 (D. Or. Nov. 6, 2019). In Caputo, the defendant was subject to computer use policies from two organizations that explicitly stated data on his computer was not private and was subject to workplace searches. Id. at *2. The defendant signed the policy at the start of his employment and was required to recertify his understanding of the policy annually. Id. In addition, the defendant was required to affirmatively check a box on a banner reiterating the policy in order to use his computer each day. Id. The court held that an expectation of privacy in the defendant's work email was objectively unreasonable because of

these workplace procedures. Id. at *3; see also United States v. Greiner, 235 F.App'x 541, 542 (9th Cir. 2007) (holding an employee lacked a legitimate expectation of privacy because his daily log-in screen contained a warning that computer files were subject to monitoring).

Here, CDSS' Privacy in the Electronic Environment policy was not communicated to employees regularly and effectively enough to diminish Aspinall's reasonable expectation of privacy. Like the defendant in Caputo, Aspinall signed his employer's privacy in the workplace policy when he onboarded at the company. (IT Acknowledgement). But while the workplace in Caputo required employees to recertify their acknowledgment of the policies annually, CDSS had no such requirement. (Aspinall Dep. 9:10-13). And unlike the employees in Caputo who were consistently reminded of their workplace's policy by a daily warning banner, Aspinall was never reminded of CDSS' policy and was thus unaware of its contents in 2023. (Aspinall Dep. 9:10-13). The singular instance in which CDSS confiscated another employee's computer six months before Aspinall's termination still did not give him sufficient reminder of these policies. (Carter Dep. 9:4-10). Though the investigation occurred during the workday, Aspinall thought the confiscated computer was CDSS property and not the employee's personal computer. (Aspinall Dep. 16:1-6).

Occasionally sharing a location or item with another employee is also insufficient to diminish an individual's legitimate expectation of privacy. United States v. Taketa, 923 F.2d 665, 673 (9th Cir. 1991). In Taketa, government officials entered one of the appellants' offices using a master key and another by force in the course of an investigation. Id. at 668. The officials possessed the master key lawfully. Id. at 673. In addition, the office that officials forcibly entered was not always locked and other officials from the same agency had occasional access to it. Id. The court held in both these instances that "privacy does not require solitude" and that other

employees' occasional access to these locked offices did not defeat the appellants' legitimate privacy interest. Id. The court also held that the appellants' privacy interest was not defeated by their failure to shut and lock the door at all times. Id.

Neither Aspinall's practice of unlocking his iPad to allow IT to run routine software updates nor Johnson's occasional use of his iPad diminished Aspinall's legitimate expectation of privacy. Just as the appellants in Taketa did not always lock their offices, Aspinall did not always have his iPad unlocked. (Aspinall Dep. 14:8-16). The officials in Taketa had lawful access to a master key just as CDSS' IT officers had Aspinall's permission to access his iPad for software updates. (Aspinall Dep. 14:8-16). And like how employees in Taketa had occasional access to one of the searched offices, so too did Aspinall's colleague Amy Johnson have occasional access to his iPad for work. (Aspinall Dep. 13:11-17). A jury could find that Aspinall maintained a reasonable expectation of privacy in his personal iPad despite CDSS' limited electronic information policy and despite his decision to unlock his device for IT to run software updates.

II. Summary Judgment Must Be Denied Because a Reasonable Jury Could Find that CDSS' Search Was Based on a Mere Hunch, Not Reasonable Suspicion, and Carter Took No Care to Avoid Viewing Personal Emails that Were Outside the Purview of the Search Despite Having Less Intrusive Options Available and No Urgent Need.

Given that Aspinall had an undiminished reasonable privacy interest, summary judgment must be denied because a reasonable jury could find that CDSS' search of Aspinall's iPad and personal email was unreasonable. The search was initiated after Carter made a logical leap about Aspinall's conduct based on rumor and a hunch about Aspinall's dinner with a guest at a work conference, and Carter took no action to attempt a less intrusive search that would have explicitly not implicated Aspinall's personal emails despite having the option and the time to do so. Public employers' intrusions on the constitutionally protected privacy interests of their employees must be judged on a standard or reasonableness under all circumstances. O'Connor, 480 U.S at 725-

726. Courts must balance the invasion into an employee's legitimate privacy expectation against the government's need for supervision and operation of the workplace. O'Connor, 480 U.S at 719-720. The search can neither have been unjustified at its inception nor unreasonable or excessively intrusive in its scope. Id. at 725-726.

Here, a jury could find Carter's search was unreasonable because Carter's hunch that Aspinall was violating CDSS' workplace policy was based merely on a rumor and knowledge of a dinner with a guest on a work trip – conduct that was on its face innocent – and because Carter had no reason to believe a search of Aspinall's iPad specifically was required to uncover evidence of such alleged misconduct. In addition, Carter's interest in searching Aspinall's device was not urgent enough to justify choosing a search method as invasive as searching his personal emails with terms reasonably likely to uncover non-work-related information. Thus, summary judgment must be denied.

A. Carter's Search Was Unjustified and Unreasonable from Its Inception Because It Was Based on a Non-Obvious Logical Leap Between a Months-Old Office Rumor And a Dinner with an Unnamed Guest

CDSS' search was not justified at its inception because it was based on Carter's inchoate and unparticularized suspicion that Aspinall and Johnson were romantically involved which was derived from an office rumor and a conference dinner expense. A search of an employee's workplace is justified only if there are reasonable grounds for suspecting that the search will turn up evidence of misconduct. O'Connor, 480 U.S at 726. Reasonableness cannot be readily determined through neat rules and must be come from a thorough review of the totality of the factual circumstances. Turiano, 562 F.Supp.3d at 277-78. Reasonable suspicion requires more than a hunch and cannot be based on inferences not drawn from articulable and specific facts. Id. at 279. Exceptions to the requirement for particularized suspicion are inappropriate when the

privacy interests implicated by the search are vast. Id. at 280.

A suspicion is not sufficiently particularized to justify a search if it is based on activity that does not constitute misconduct and is not directly related to alleged misconduct. Turiano, 562 F.Supp.3d at 279. In Turiano, a police department sought to access data from an officer's personal cell phone pursuant to an internal investigation related to a violent protest. Id. at 268. The plaintiff testified under oath that he discussed the protest in text messages. Id. Speaking about a protest on its own, however, did not constitute misconduct in the plaintiff's workplace even though it was ostensibly connected to the search's purpose. Id. The court held that suspicion that the search would uncover evidence that the plaintiff texted about the protest was insufficient to justify a search aimed at uncovering information about a related but distinct matter. Id. See also Taketa, 923 F.2d at 674 (finding that a search was justified at inception because a colleague reported potential misconduct directly related to the item searched).

Here, Carter's suspicion was spurred by an expense report line item for a dinner at a work conference with an unnamed guest – activity that did not constitute misconduct and was not directly related to allegations of a workplace relationship. ("Expense Report"). Aspinall's conduct was loosely related to the subject of Carter's inquiry of a romantic relationship just as the search in Turiano was loosely related to the subject matter of the protest. (Carter Dep. 8:5-18). Like the texts from the plaintiff in Turiano that were not on their own misconduct, a reasonable jury could find that Aspinall's eating with a guest at a work conference was neither misconduct nor out of the ordinary. (Aspinall Dep. 17:17-20). While Carter also in part based his search on the rumors from another employee at CDSS, this case is distinguishable from Taketa because, unlike those employers who initiated an investigation immediately upon hearing the report of alleged misconduct, Carter did not deem the information sufficiently important to begin

an investigation for several months. (Carter Dep. 4:13-17, 8:1-7).

B. Carter's Search Was Unreasonable in Scope Because He Did Not Take Any Measures to Avoid Searching Personal Emails and The Investigation Did Not Concern a Matter of Sufficient Urgency to Justify Utilizing An Intrusive Search Method.

Even if the search was justified at its inception, a reasonable jury could still find CDSS' search of Aspinall's email account was unreasonable in scope because the objectives of his search did not require reviewing personal emails and was not of an urgent enough need to justify Carter's refusal to wait several days for IT's search of CDSS' work servers to be completed. A search is unreasonable in scope if the measures adopted are not reasonably related to the objectives of the search or if they are excessively intrusive in light of the circumstances giving rise to the search. Quon, 560 U.S. at 761. Because of the sheer amount of personal data held on a cell phone, even a restricted search of such a device would likely impose "few meaningful constraints" on the scope of a data that could be uncovered. Riley, 573 U.S. at 399.

An employer's search is unreasonable in scope when it chooses a highly intrusive method despite having less intrusive options that could similarly accomplish their objectives. Hibbert v. Schmitz, No. 16-CV-3028, 2019 WL 8405217, at *17 (C.D. Ill. Feb. 7, 2019); see Quon, 560 U.S at 761-763 (stating that the level of intrusiveness must be proportional to the search's objectives even if employers are not required to use the least intrusive method available to them). In Hibbert, an employer searched an employee's cell phone to uncover evidence of an inappropriate workplace relationship. Id. at *16. The investigator aimed to retrieve all text messages sent by the plaintiff, not just messages between the plaintiff and her alleged partner. Id. Because of a security measure on the plaintiff's phone that barred access to text messages, the investigators searched plaintiff's photos, contacts, and a messenger app. Id. at *17. The defendants opted to search the plaintiff's cell phone rather than reviewing camera footage or

interviewing her, her partner, or witnesses. Id. at *17. The court held that a reasonable trier of fact could find the search to be unreasonable in scope because the defendants chose a much more intrusive search method than was warranted to accomplish their objectives. Id. See also Larios v. Lunardi, 445 F. Supp. 3d 778, 784 (E.D. Cal. 2020), aff'd, 856 F. App'x 704 (9th Cir. 2021) (holding that a search is unreasonable in scope when it includes a volume of data disproportionate to the needs of the investigation, even if investigators first attempted less intrusive methods first).

Here, Carter had various options for how to proceed with his investigation and chose a far more intrusive type of search than was required by his objectives. Just as the defendant in Hibbert chose an invasive cell phone search over interviewing the alleged couple or witnesses, so too did Carter choose to conduct a search of Aspinall's iPad rather than speaking directly with him or Johnson, as he later did. (Carter Dep. 15:18-20). Carter also had the option to use traditional channels to search only CDSS' servers for evidence of a relationship, just as the defendants in Hibbert had the option to review camera footage to corroborate their suspicions. (Carter Dep. 11:1-4). And while Carter's search of Aspinall's iPad was more targeted than the Hibbert employer's broad review of the plaintiff's cell phone contents, it too did not limit its scope only to conversations between Aspinall and Johnson but instead cast a wide net for all messages in a two-month span including the words "Amy" or "Johnson" and referencing "dinner," "AGSSP," or "Santa Barbara." (Carter Dep. 12:8-11). A reasonable jury could interpret this search, in light of the other options available to Carter, as one more intrusive than was required for his objectives.

An intrusive search is outside the bounds of reasonableness unless an employer takes care to avoid reviewing personal items while searching for evidence of workplace misconduct.

Espinoza, 2018 WL 2318335 at *6. In Espinoza, defendants searched an employee's desk for non-investigative workplace purposes. Id. During the search, defendants relocated the plaintiff's personal items to a box prior to conducting their search. Id. The court held that the search was reasonable in scope in part because the defendants limited their search explicitly to work-related materials. Id.; see also Quon, 560 U.S at 762 (noting that petitioners limited the scope of their search by redacting all messages sent by respondent while off-duty from their report to reduce the amount further review would intrude on his private messages).

Here, Carter made an affirmative choice to conduct a search that would uncover Aspinall's personal emails. (Carter Dep. 14:16-19). Unlike the defendants in Espinoza who took care to only search work-related materials, Carter declared he "wasn't concerned" that he would be searching Aspinall's personal email account. (Carter Dep. 14:16-19). Carter then utilized the personal email messages he uncovered in his search, unlike the petitioners in Quon who limited their search by redacting private off-duty messages from their report. (Carter Dep. 13:18-14:1).

Absent an urgent need to protect health and safety, a broad and overly intrusive search is unreasonable. Redding v. Safford Unified Sch. Dist. #1, No. CV 04-265-TUC-NFF, 2005 WL 8165048, at *10 (D. Ariz. Mar. 18, 2005). In Redding, school officials conducted strip searches of several students in order to find illicit pills that were being used throughout the school. Id. Defendants claimed that the strip search was necessary because there was an urgent need to find the pills quickly before students had a chance to ingest them. Id. The court found the searches reasonable in scope because of the school's urgent need to discover all illicit pills on the premises. Id.; see also Larios v. Lunardi, 442 F. Supp. 3d 1299, 1310 (E.D. Cal. 2020), aff'd, 856 F. App'x 704 (9th Cir. 2021) (holding that a search investigating an unauthorized relationship was reasonable in scope because the relationship had given rise to a domestic violence incident

that jeopardized the safety of the plaintiff's affair partner).

Here, there was no imminent health or safety threat that justified Carter's choice to conduct an intrusive iPad search rather than waiting for the results of CDSS' server search. Unlike in Redding in which a thorough search would uncover illicit pills and preclude a future harm, here the record does not indicate that there was a pressing interest in uncovering Aspinall and Johnson's consensual relationship immediately. (Carter Dep. 8:1-3). In fact, Carter had taken no action on workplace rumors that Aspinall and Johnson were romantically involved for three months. (Carter Dep. 8:1-3). And unlike the imminent danger of a domestic violence situation in Larios, there was no foreseeable danger to Aspinall or Johnson – who were in a consensual relationship at this point in time – if Carter waited for the server search results. (Aspinall Dep. 5:15-6:2). Even if this court decided the government's interests required Carter to utilize a more immediate search method, however, Carter maintained the option to speak directly to Aspinall and discover if he and Johnson were in a relationship – which he later did. (Carter Dep. 10:14-15, 15:18-22). A reasonable jury considering the totality of the circumstances could find that Carter's search was neither justified at inception nor reasonably limited in scope in light of the privacy concerns implicated by allowing unwarranted access to government employees' devices.

CONCLUSION

The defendants are not entitled to judgment as a matter of law because a reasonable jury could conclude that Ellis Carter's search of Nathan Aspinall's personal iPad and personal email account unreasonably intruded on Aspinall's expectation of privacy and thus triggered his constitutional right against unwarranted searches and seizures. Personal electronic devices like cell phones and iPads contain vast amounts of data and personal information, far more than that of items like wallets and purses. Aspinall had a constitutionally cognizable privacy interest at

stake because his expectation of privacy in a device he purchased for himself for personal use and kept password protected was undiminished by a workplace electronic privacy policy that was not sufficiently communicated to its employees and permitted review of only work-related information under limited circumstances. In light of Aspinall's privacy interest, Carter's search was not justified at its inception by a particularized reasonable suspicion but was instead the result of a hunch based on office rumor and an expense report line item that was on-its-face innocent. Finally, Carter's search of Aspinall's comingled email accounts, despite its targeted terms, was more intrusive than required by a non-urgent workplace misconduct investigation. Because this two-prong test is both fact-intensive and implicates a novel privacy interest in a new digital age, this matter is unsuited for summary judgment and the motion must be denied.

DATED: April 14, 2024

Respectfully Submitted,
LINDELL, DUNCAN & DIAZ LLP

/s/ Lia Rocchino
Lia Rocchino
501 Market Street
Riverside, CA 92501

Attorney for the Plaintiff.
Nathan Aspinall

CERTIFICATE OF SERVICE

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

Susan Smith
Gowen, Pierce and Simon LLP
1375 East 9th Street
Riverside, CA 92501
Attorney for Defendant

/s/ Lia Rocchino
Dated: April 14, 2024