Meeghan Dooley
DUNCAN, GOWEN, & FIROZ LLP
501 Market Street
Riverside, CA 92501

Attorneys for Praveen Patel

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

PRAVEEN PATEL,	:	
	:	
Plaintiff	:	**No. 20-CV-0447 JGB**
	:	
v.	:	
	:	
JEFFREY POPOVIZ, in his individual capacity,	:	
	:	
	:	
Defendant.	:	
	:	

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

SUPREME COURT CASES

COURT OF APPEALS CASES

DISTRICT COURT CASES

OTHER AUTHORITIES

INTRODUCTION

Technological innovations have reshaped workplace norms by enabling employees to use their personal electronic devices for work-related purposes, giving rise to an important question: to what extent those employees' electronic devices are protected from government intrusion under the Fourth Amendment.

Fourth Amendment cases once only involved searches of items that held a finite amount of information. Now, courts are faced with cases involving searches of electronic devices that put seemingly limitless amounts of information in the hands of potential searchers. The average laptop, for example, allows individuals to hold 200 million pages of information – enough to fill five floors of an academic library – in one hand. The owners of these devices often use them to store extensive amounts of personal information. When they use these same devices to increase efficiency at work, they risk being subjected to intrusive privacy violations by their employers under the guise of an allegedly reasonable Fourth Amendment search. Caution must be used when determining whether these searches can proceed.

Praveen Patel was subjected to one such search. A hardworking Director at the California Department of Social Services ("CDSS"), Patel bought an iPad for his personal use. In order to work after hours and stay up to date on work trips, he configured the iPad to send and receive emails from his work account in addition to his personal account. Patel was cautious to keep private activities separate from any work he completed on his iPad.

Pursuant to company policy, Patel left his iPad with CDSS's IT department and temporarily removed its password so IT staff could install software updates. After learning that Patel's iPad was temporarily unprotected, Jeffrey Popoviz, Director of Personnel Management, seized the opportunity to begin an investigation into Patel's personal life. He requested that the

IT department conduct a search of the emails on Patel's iPad. Although Popoviz was warned that a search of Patel's iPad would include emails from both his personal and work accounts, Popoviz proceeded with the search.

Popoviz is not entitled to summary judgment because he cannot establish as a matter of law that the search he conducted was reasonable. Patel's iPad and Gmail account were protected under the Fourth Amendment because he had a legitimate expectation of privacy in his personal iPad. A reasonable jury could conclude that Patel's Fourth Amendment rights were violated when Popoviz conducted his search. Accordingly, summary judgment must be denied.

STATEMENT OF MATERIAL FACTS

Praveen Patel joined CDSS as the Director of the Youth and Family Services Division in January 2018. (Patel Dep. 3:2-10, 6:4-6, attached as Exhibit ("Ex.") A). His primary role was to oversee child welfare services. (Patel Dep. 3:7-10). Patel was the dedicated leader of twenty staff members and three Deputy Directors, including his now-fiancé, Anna Wolfe. (Patel Dep. 3:11-4:5, 5:15-6:2).

Patel bought an iPad for his personal use prior to joining CDSS. (Patel Dep. 11:4-7). When he was hired as a Director, CDSS provided Patel with a desktop computer. (Patel Dep. 6:7-11, 11:4-5). CDSS also expressly permitted employees to use their personally owned mobile computing devices for work-related purposes. (Popoviz Dep. 15:1-3, attached as Ex. B). Patel configured his iPad to send and receive CDSS emails so he could work after hours and stay updated on work trips. (Patel Dep. 11:8-13, 12:1-4). Patel also continued to use his iPad for a wide range of personal activities. (Patel Dep. 12:5-8).

Patel was provided with CDSS's Information Technology Policies upon hiring. (Patel Dep. 10:1-11; CDSS's Information Technology Policies ("CDSS IT Policies"), attached as Ex.

C; Acknowledgement and Receipt of CDSS's Information Technology Policies, dated Jan. 12, 2018, attached as Ex. D). The first policy concerned privacy in the electronic environment and granted CDSS access only to that electronic information that was work-related. (CDSS IT Policies, at 1). The second policy, regarding mobile-computing devices, listed requirements for employees who conducted CDSS-related work on their personal electronic devices. (CDSS IT Policies, at 1-2). The policy made clear that CDSS would not provide an allowance or reimbursement for employees' personally owned devices. (CDSS IT Policies, at 1). It required employees who used their personal devices for work to grant CDSS's IT unit access to their devices for the limited purposes of "install[ing] software updates, as needed, and CDSS-issued tracking and recovery software to facilitate its return if lost or stolen." (CDSS IT Policies, at 2). No other language in CDSS's technology policies granted anyone at CDSS access to employees' personal electronic devices for any reason. (CDSS IT Policies).

While a display option on the iPad allows users to view emails from multiple accounts on one screen, Patel was careful to keep the contents of his CDSS and Gmail accounts separate. (Patel Dep. 12:13-19). Patel never sent a personal email from his CDSS email account. (Patel Dep. 13:2-5). Patel maintained possession of his iPad with the limited exceptions of loaning it once or twice to Anna Wolfe while IT worked on her computer and occasionally leaving it with the IT department for software updates pursuant to company policy. (Patel Dep. 13:11-14:5; CDSS IT Policies, at 2).

In June 2020, Patel and CDSS's other senior department personnel attended an industry conference in Santa Barbara. (Patel Dep. 17:1-7). While at the conference, Patel often had dinner with members of his team, including one evening with Anna Wolfe. (Patel Dep. 17:8-11).

Patel later sought reimbursement from CDSS for expenses that he incurred at the conference. (Patel Dep. 17:17-20).

Upon his return to the office, Patel left his iPad with the IT department because he received notice that it was due for updates. (Patel Dep. 14:6-10). Patel's iPad was password protected. (Patel Dep. 11:14-15). The IT staff did not have Patel's password, so he unlocked it temporarily to allow them to install the updates. (Patel Dep. 14:11-16).

That same day, Jeffrey Popoviz, CDSS's Director of Personnel Management, reviewed Patel's expense report from the conference. (Popoviz Dep. 3:17-19, 8:6-7, 8:20-9:2, 9:16-10:3). Although it was normal for Patel to eat with his colleagues at work conferences, Popoviz found one entry unusual because it reflected the dinner for two. (Patel Dep. 17:8-11; Popoviz Dep. 8:6-15). Three months earlier, Popoviz learned that Patel might be in a relationship with Ms. Wolfe in contravention of company policy. (Popoviz Dep. 5:3-6, 6:19-22). He did not inquire further at the time. (Popoviz Dep. 7:22-8:3).

Popoviz saw Patel in the office several times that day. (Popoviz Dep. 10:9-13). He chose not to ask about the expense report. (Popoviz Dep. 10:9-13). Instead, Popoviz immediately called IT to ask if the IT staff could search Patel's email account. (Popoviz Dep. 8:20-9:2; 10:14-18). He did not inform Patel or ask Patel's permission. (Popoviz Dep. 10:14-18). The IT officer on duty told Popoviz that she could search CDSS's servers for work emails. (Popoviz Dep. 10:5-6). She also informed Popoviz that, fortuitously for him, Patel had left his personal iPad with IT earlier that morning for software updates. (Popoviz Dep. 10:1-3; Patel Dep. 14:6-10). She noted that Patel's iPad was normally password protected, but that he unlocked it to allow her to install the updates. (Popoviz Dep. 10:1-8; Patel 14:15-16).

Popoviz seized the opportunity. (Popoviz Dep. 11:6-7). He provided the IT officer with a list of search terms and instructed her to run the searches ASAP. (Popoviz Dep. 11:6-7, 12:8-11). He also asked her to make copies of any emails captured by the searches. (Popoviz Dep. 12:8-11). Before running the search of Patel's iPad, the IT officer warned Popoviz that it would include emails from Patel's personal Gmail account in addition to his CDSS account. (Popoviz Dep. 14:2-19). Without hesitation, Popoviz sanctioned the search. (Popoviz Dep. 14:16-19).

As predicted, the results from Popoviz's search captured emails from Patel's personal Gmail account. (Popoviz Dep. 13:9-19). Those emails contained private, non-work related communications between Patel and Anna Wolfe. (Patel Dep. 18:13-16; Popoviz Dep. 13:9-19; Emails between Praveen Patel and Anna Wolfe, attached as Ex. E). The search of CDSS's network did not. (Popoviz Dep. 13:20-14:1).

Patel was shocked and furious to learn that Popoviz "abuse[d] [his] trust" and searched his personal iPad and Gmail account. (Patel Dep. 14:17-15:6). He had no idea that by leaving his iPad with the IT department, the IT staff or Popoviz would have access to his Gmail account. (Patel Dep. 14:17-15:10). While Patel was aware of an earlier event in which Popoviz forcefully entered a CDSS employee's office and searched his laptop, Patel assumed the laptop searched was a work laptop. (Patel Dep. 15:11-16:3; Popoviz Dep. at 9:4-15). It was not. (Patel Dep. 16:4-5). Patel referred to the search of his personal iPad and Gmail account as "unconscionable." (Patel Dep. 15:4-6). Shortly after the search, Popoviz terminated Patel's employment with CDSS. (Popoviz Dep. 16:11-18).

SUMMARY JUDGMENT STANDARD

Summary judgment may only be granted if a movant establishes that there is no genuine dispute as to any material fact and he is entitled to judgment as a matter of law. Fed. R. Civ. P.

56(a). The moving party bears the burden of identifying materials in the record that show the absence of a genuine dispute of material fact. Fed. R. Civ. P. 56(c)(1)(A); see also Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986). All reasonable inferences must be drawn in favor of the non-moving party. See Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 255 (1986). If the movant cannot establish a genuine dispute of material fact – "that is, if the evidence is such that a reasonable jury could return a verdict for the nonmoving party" – summary judgment must be denied. Id. at 248.

ARGUMENT

Popoviz is not entitled to summary judgment because Patel had a legitimate expectation of privacy in his personal iPad and Gmail account and a reasonable jury could find that Popoviz's search violated Patel's Fourth Amendment rights. Under the Fourth Amendment, individuals have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. This protection extends to searches conducted by government employers. See O'Connor v. Ortega, 480 U.S. 709, 717 (1987) ("[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer"). In O'Connor v. Ortega, the Supreme Court outlined the proper framework for determining whether a government employer's search was constitutional. Id. at 717-19, 725-26. First, a court must determine if the government employee's Fourth Amendment rights were implicated. Id. at 715. If the employee had a reasonable expectation of privacy in his private property based on the "operational realities of the workplace," that property is protected under the Fourth Amendment. Id. at 717-18. Once a reasonable expectation of privacy has been established, the court must determine whether the search itself was constitutional. Id. at 725. When a government employer conducts a search for

a work-related, non-investigatory purpose or to investigate employee misconduct, the "special needs" of the workplace render obtaining a warrant burdensome and impracticable. Id. at 722, 725. Therefore, a warrant is not required. Id. Instead, once a legitimate expectation of privacy has been established, the constitutionality of the search is determined by a standard of reasonableness. Id. at 725.

The court's analysis must take into account the type of property searched, particularly in cases where that property is an electronic device. See United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013); see also Kyllo v. United States, 533 U.S. 27, 33-34 (2001) ("[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology"). Technological advancements have allowed more employees to use their personal electronic devices for work-related activities. See City of Ontario v. Quon, 560 U.S. 746, 759 (2010). As society's reliance on electronic devices has grown, the Supreme Court has expressed increasing concern regarding individuals' privacy in their electronic devices. See Riley v. California, 573 U.S. 373, 393 (2014). Whereas cell phones – or "minicomputers," as the Court more aptly calls them – were once a rare commodity, they now are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." Id. at 385. Cell phones "place vast quantities of personal information literally in the hands of individuals." Id. at 386; see also Cotterman, 709 F.3d at 964 ("The average 400-gigabyte laptop hard drive can store over 200 million pages – the equivalent of five floors of a typical academic library"). Because of this, searches of electronic devices have the capacity to reach considerably more information than searches of other types of property. Riley, 573 U.S. at 396-97. As the Court points out:

> [A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many

> sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form – unless the phone is.

Id. While "a firm line at the entrance of a house" has been drawn to protect the privacy of one's home under the Fourth Amendment, see Kyllo, 533 U.S. at 39, changes in societal norms have prevented the Court from establishing a similar line for an electronic device, see Quon, 560 U.S. at 759. That determination instead must be made on a case-by-case basis using a standard of reasonableness. See O'Connor, 480 U.S. at 718, 725. Wherever the line in this case is drawn, a reasonable jury could conclude that Popoviz crossed it. Patel had a legitimate expectation of privacy in his personal iPad and Gmail account that caused them to be protected under the Fourth Amendment. Because Popoviz cannot show as a matter of law that his search was reasonable under the Fourth Amendment, summary judgment must be denied.

I. PATEL'S EXPECTATION OF PRIVACY IN HIS PERSONAL IPAD AND GMAIL ACCOUNT WAS REASONABLE AS A MATTER OF LAW BECAUSE HE MANIFESTED A SUBJECTIVE EXPECTATION OF PRIVACY THAT SOCIETY WOULD RECOGNIZE AS OBJECTIVELY REASONABLE.

Patel had a legitimate expectation of privacy because his actions and the circumstances under which they were taken demonstrate a subjective expectation of privacy in his personal iPad and Gmail account that society would recognize as objectively reasonable. In O'Connor, the plurality stated that a government employee's protection under the Fourth Amendment extends to searches of any private property in which the employee has a reasonable expectation of privacy. O'Connor, 480 U.S. at 715 (plurality opinion). Eight justices agreed that the reasonableness of that expectation should be assessed based on the "operational realities of the workplace." Id. at 717 (plurality opinion); id. at 737 (Blackmun, J., dissenting). [1] An individual

[1] Justice Scalia, in his concurring opinion, suggested that rather than reviewing the "operational realities of the workplace" to determine whether an employee has a reasonable expectation of privacy, "the offices [and items within them] of government employees . . . are governed by Fourth Amendment protections as a general matter." O'Connor, 480 U.S. at 731 (Scalia, J., concurring in judgment). The Court has not

has a legitimate expectation of privacy if he demonstrates a subjective expectation of privacy in an item or area and that expectation is one "that society would recognize as objectively reasonable." United States v. Sarkisian, 197 F.3d 966, 986 (9th Cir. 1999). The record establishes that Patel had a subjective expectation of privacy in his personal iPad and Gmail account. Patel was careful not to send work emails through his personal Gmail account. (Patel Dep. at 13:4-5). See Trujillo v. City of Ontario, 428 F. Supp. 2d 1094, 1102 (C.D. Cal. Apr. 14, 2006) (holding that an individual manifests a subjective expectation of privacy if he makes efforts to preserve something as private). He also kept a password on his iPad. (Patel Dep. at 11:14-15; 14:8-14). See United States v. Ziegler, 474 F.3d 1184, 1189 (9th Cir. 2007) (holding that a password on plaintiff's computer was sufficient evidence of a subjective expectation of privacy). By making an effort to keep his personal and work email accounts separate and protecting his iPad with a password, Patel manifested a subjective expectation of privacy.

Patel's subjective expectation of privacy was objectively reasonable because the pervasive nature of electronic devices and manner in which Patel used his personal iPad would lead society to consider them protected from government intrusion. While there is "no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable," factors that often are considered include the Framers' intent when drafting the Fourth Amendment, society's views about what should be protected from government intervention, and the manner in which an employee used the property. O'Connor, 480 U.S. at 715. The Ninth Circuit has interpreted the inclusion of "papers" in items protected under the Fourth Amendment to reflect the Framers' "deep concern with safeguarding the privacy of

clarified which threshold test is correct. Quon, 560 U.S. at 757. However, because Justice Scalia's concurrence proposed that a government employee's property is covered under the Fourth Amendment as a general matter, Patel's iPad would be protected under Justice Scalia's approach and it need not be discussed further.

thoughts and ideas . . . from invasion by the government." Cotterman, 709 F.3d at 964. The Ninth Circuit specifically related this safeguard to electronic devices and their contents: "iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records *and private emails*. This type of material implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers.'" Id. (emphasis added). Additionally, society expects electronic devices and their contents to remain private. See id. at 966. ("[T]he uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy"). While this expectation can be affected by the "operational realities of the workplace," the Supreme Court has held that "not everything that passes through the confines of the business address can be considered part of the workplace context." O'Connor, 480 U.S. at 715-17. An employee's expectation of privacy in the outside of a briefcase, for example, might change once it is brought into the office, but the same is not true for the contents of the briefcase. Id. at 716. Although Patel brought his iPad to the office, he used his iPad and personal Gmail account in a manner that society would expect to remain private. Patel's expectation of privacy in his personal iPad and Gmail account was reasonable as a matter of law because (1) he exercised exclusive control over the iPad and used it to store personal information, (2) merely allowing the IT department or an occasional colleague to access his iPad for limited purposes did not destroy that expectation, and (3) no company regulation provided Popoviz access to Patel's personal iPad or Gmail account.

A. Patel had a reasonable expectation of privacy in his iPad because he used his iPad exclusively and stored personal information on it.

A government employee's expectation of privacy is reasonable if he uses the property exclusively and stores personal items inside it. See O'Connor, 480 U.S. 709, 718-19. In

O'Connor, the plaintiff worked at a state hospital. Id. at 712. His office, desk, and file cabinet were searched as part of an investigation. Id. at 712-13. The search uncovered a Valentine's Day card, photograph, book of poetry, and other personal items that belonged to the plaintiff. Id. at 714. The Court noted that hospital staff might have had an occasional need to access the office. Id. at 718. It held that regardless of whether or not hospital staff entered his office, the plaintiff had a reasonable expectation of privacy in his desk and file cabinet because they were used by him exclusively, he did not share his office with other employees, and he kept personal items inside them. Id. at 718-19.

Patel had a reasonable expectation of privacy in his personal iPad because he had exclusive use of the iPad and stored personal information on it, including the contents of his Gmail account. Like the plaintiff in O'Connor, who did not share his office with other employees, Patel had exclusive use of his iPad at work. Also like the circumstances in O'Connor, in which hospital staff occasionally entered the plaintiff's office, Patel occasionally loaned his iPad to a colleague or left it with the IT department for software updates. (Patel Dep. 13:11-14). Patel's iPad, like the desk and file cabinet in O'Connor, contained personal items, such as private communications he sent and received through his Gmail account. (Patel Dep. 11:4-7; 12:5-8). Patel had a reasonable expectation of privacy in his iPad because he retained exclusive use of the iPad and used it to store personal information.

While the Supreme Court in O'Connor analyzed an expectation of privacy in items that can hold a finite amount of information, the Court in City of Ontario v. Quon addressed an employee's expectation of privacy in an electronic device. See Quon, 560 U.S. at 759. In Quon, the plaintiff claimed that he had a reasonable expectation of privacy in personal text messages sent from an employer-provided pager. Id. at 750. Although the Court did not reach a

conclusion regarding the plaintiff's expectation of privacy, it discussed the difficulty of predicting how "rapid changes in the dynamics of communication and information transmission . . . in technology" might affect an employee's expectation of privacy and whether it was one society would accept as reasonable. Id. at 751, 759. Presenting arguments for both sides, the Court noted that a person might have a strong expectation of privacy in a technological device because "cell phone and text message communications are so pervasive that some persons may consider them to be essential means…for self-expression." Id. at 760. The Court continued, "On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who needs cell phones or similar devices for personal matters can purchase and pay for their own." Id. Both sides of the Supreme Court's argument support the conclusion that Patel had a reasonable expectation of privacy in his personal iPad and Gmail account. Patel used his iPad for pervasive and private communications, which he sent and received through his Gmail account. (Patel Dep. 18:13-16). Patel also purchased his iPad and received no reimbursement from CDSS. (Patel Dep. 11:5-7; CDSS IT Policies, at 1). Both arguments support an expectation of privacy that society would consider reasonable.

B. Patel's expectation of privacy in his iPad was not destroyed merely because the IT department or a colleague occasionally had access to it.

A government employee's reasonable expectation of privacy in property does not become unreasonable merely because other employees have access to that property. See Richards v. County of Los Angeles, 775 F. Supp. 2d 1176, 1183 (C.D. Cal. Mar. 1, 2011). In Richards, the plaintiff, a dispatcher for the government, was videotaped in the dispatch room during an investigation into employee misconduct. Id. at 1179. The plaintiff engaged in several private, non-work related activities in the dispatch room and it contained objects normally reserved for use at home, including a television and cooking supplies. Id. at 1183. The room was secured by

restricted access doors. Id. The court rejected an argument that the plaintiff's expectation of privacy in the room was unreasonable because security officers and supervisors had access to it and it was shared by multiple employees. Id. Instead, the court held that the plaintiff's expectation of privacy was reasonable because the contents of the dispatch room supported its characterization as private and the occasional entry of supervisors did not destroy that expectation. Id.; see also O'Connor, 480 U.S. at 718 (holding that the hospital staff's ability to access to the plaintiff's office did not make it "so open to fellow employees or the public that no expectation of privacy [was] reasonable").

Patel's expectation of privacy in his iPad did not become unreasonable simply because he left it with the IT department or occasionally loaned it to a colleague. Like the plaintiff in Richards, who expected privacy in the dispatch room because he used it for private activities in addition to work, Patel had an expectation of privacy in his personal iPad because he used it for personal activities, like sending communications through his Gmail account. (Patel Dep. 11:5-7, 12:7-8). Also, like the dispatch room in Richards, which was secured by restricted access doors, Patel's iPad was secured by a password. (Patel Dep. 11:14-15). Both the dispatch room in Richards and Patel's iPad could be accessed by other employees, but the ability of other employees to access Patel's iPad was limited to the rare circumstance in which he lent it to a colleague or left it with the IT department for updates. (Patel Dep. 13:11-14, 13:18-14:5). As in Richards, the limited ability of other CDSS employees to access his iPad with his permission did not destroy Patel's expectation of privacy in his personal iPad and Gmail account.

C. The absence of a regulation or policy authorizing CDSS to search Patel's personal electronic devices establishes that Patel's expectation of privacy in his iPad and Gmail account was reasonable.

The absence of a regulation or policy expressly granting a government employer permission to search an item indicates that an employee will have a reasonable expectation of privacy in that item. See, United States v. Bunkers, 521 F.2d 1217, 1221 (9th Cir. 1975). In Bunkers, the plaintiff postal worker's locker was searched by her employer while investigating missing parcels. Id. at 1219. The locker was the property of the government. Id. The plaintiff accepted use of the locker subject to published regulations allowing her employer to search the locker upon suspicion of criminal activity. Id. at 1220-21. The court held that the plaintiff's expectation of privacy was unreasonable because she agreed to regulations allowing her employer to search the property. Id.; see also Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1335 (9th Cir. 1987) ("[an employee] would enjoy a reasonable expectation of privacy in areas given over to his exclusive use, unless he was on notice from his employer that searches of the type to which he was subjected might occur from time to time for work-related purposes").

Patel's expectation of privacy was reasonable because no company regulation or policy granted Popoviz permission to search Patel's personal iPad or Gmail account, and the technology policies that did exist limited access of its employees' personal electronic devices to the IT department for a limited set of purposes. Unlike the employer in Bunkers, who provided the plaintiff with published regulations permitting a search of her locker, CDSS did not impose any regulation or policy granting at CDSS the right to search Patel's iPad. (CDSS IT Policies). The first technology policy, titled "Privacy in the Electronic Environment," gave CDSS the right to review *work-related* electronic information. (CDSS IT Policies, at 1). Patel's Gmail account was not work-related: it contained private communications, was stored on Patel's personal iPad, and was not connected to the CDSS servers. (Patel Dep. 18:13-14; Popoviz Dep. 13:9-11, 13:18-14:1). The second policy, the "Mobile-Computing Device Policy," established regulations for

employees' personally owned devices. (CDSS IT Policies, at 1-2). The policy expressly limited access of employees' personal electronic devices to the IT department and specified that access was granted solely to "install software updates, as needed, and CDSS-issued tracking and recovery software to facilitate its return if lost or stolen." (CDSS IT Policies, at 2). No other provision in CDSS's technology policies referenced its ability to access employees' personal communications or electronic devices. (CDSS IT Policies). By permitting the IT unit to access an employee's personal electronic device and listing the specific purposes for which it could do so, CDSS expressly limited its access of employees' electronic devices to IT for those purposes. (CDSS IT Policies). No regulations or policies granted Popoviz or any other CDSS employee the right to search Patel's personal iPad and Gmail account, so Patel's expectation of privacy was reasonable.

II. POPOVIZ IS NOT ENTITLED TO SUMMARY JUDGMENT BECAUSE A REASONABLE JURY COULD FIND THAT THE SEARCH WAS EXCESSIVELY INTRUSIVE AND NOT REASONABLY RELATED IN SCOPE TO THE OBJECTIVES OF THE SEARCH.

A reasonable jury could find that Popoviz's search was unreasonable because the measures taken were not reasonably related to the objectives of the search and because the search was excessively intrusive. In O'Connor, the plurality held that once a reasonable expectation of privacy has been established, the constitutionality of a government employer's search is determined by a standard of reasonableness. O'Connor, 480 U.S. at 726. [2] It specified that a

[2] Justice Scalia's concurring opinion departed from the plurality's two-factor reasonableness standard and instead suggested that a public employer's search is constitutional if it is "to retrieve work-related materials or to investigate violations of workplace rules," as would be reasonable in the private-employer context. O'Connor, 480 U.S. at 732. The Ninth Circuit has overwhelmingly followed the two-factor reasonableness standard outlined in Justice O'Connor's plurality opinion. See, e.g. Schowengerdt, 823 F.2d at 1335; United States v. Taketa, 923 F.2d 665, 673-74 (9th Cir. 1991); Khachatourian v. Hacienda La Puente Unified School District, 572 Fed.Appx 556, 558 (9th Cir. 2014); Nickler v. County of Clark, 752 Fed.Appx. 427, 430 (9th Cir. 2018). Therefore, the plurality's approach is controlling and will be discussed in detail here.

government employer's search for work-related, non-investigatory reasons or to investigate employee misconduct is reasonable only if it is both justified at its inception and "reasonably related in scope to the circumstances which justified the interference in the first place." Id. at 725-26 (quoting New Jersey v. T.L.O., 469 U.S. 325, 341 (1985)). If a search fails to meet either requirement, it is unreasonable and violates the employee's Fourth Amendment rights. Id. at 725-26. A search is justified at its inception if "there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct." Id. at 726. Patel does not contest that a search would have been justified if it was reasonably related in scope to the purposes of the search; however, Popoviz cannot show that his search was reasonable as a matter of law. The scope of a search is reasonable only if the measures used are sufficiently related to the objectives of the search and not excessively intrusive. Id. at 726. Courts must consider the "circumstances that [gave] rise to the search" to determine whether the measures taken were reasonably related to the purpose of the search. Larios v. Lunardi, 445 F.Supp.3d 778, 783 (E.D. Cal. 2020), *appeal docketed on other grounds*, No. 20-15764 (9th Cir. Apr. 23, 2020) (citing Quon, 560 U.S. at 761-62). A search is excessively intrusive if it is not "commensurate with the seriousness of the suspected misconduct." Richards, 775 F. Supp. 2d at 1184. A reasonable jury could find that Popoviz's search of Patel's personal iPad and Gmail account was not reasonably related to the scope of the search because (1) it exceeded the measures necessary to achieve the objective of the search; (2) was likely to reveal private details of Patel's life due to Patel's significant expectation of privacy in his iPad, and (3) less intrusive methods were readily available.

A. Popoviz's search of the Gmail account was not reasonably related in scope to the objectives of the search because by searching emails in Patel's personal Gmail account, Popoviz's investigation exceeded the methods permitted by CDSS's information technology policies.

An employer's search methods are not reasonably related in scope to the objectives of the search if they exceed those expressly granted to him. See Larios, 445 F. Supp. 3d at 784. In Larios, the plaintiff, a highway patrol officer, was suspected of employee misconduct. Id. at 784. Pursuant to a policy requiring employees to turn over work product on their personal devices, the defendant took the plaintiff's cell phone to conduct a forensic extraction of his work product. Id. at 783-84. After a limited extraction of work product alone was unsuccessful, the defendant ordered a backup of the entire phone. Id. at 783. The court held that the search was unreasonable because the employer seized more than the work-related messages allowed by the policy and the need did not justify the means. Id. at 784-85. Reasoning that a phone's storage capacity creates a potentially limitless intrusion into a person's private life, the court noted that while the extraction of work product based on customized data withdrawal would have been reasonable, a backup of the entire phone was not. Id.

Popoviz's search was not reasonably related to the objectives that gave rise to it because his search of Patel's private Gmail account exceeded the methods available to him under CDSS's information technology policies. Like the defendant in Larios, who sanctioned the backup of the plaintiff's phone but did not create the backup himself, Popoviz sanctioned the search of Patel's private email account. (Popoviz Dep. 9:17-10:6). Popoviz had the option to search only Patel's work email consistent with CDSS's technology policies, which granted the company access to its employees' work-related electronic information. (Popoviz Dep. 9:17-10:6; CDSS IT Policies, at 1). However, instead of conducting a search within those boundaries, Popoviz sanctioned a search that he knew would include emails in Patel's private Gmail account. (Popoviz Dep. 14:2-17). Although Popoviz provided search terms to narrow the results, the search terms targeted results in Patel's personal Gmail account, which he was not given access to under CDSS's own

policies and therefore still exceeded appropriate measures. (Popoviz Dep. 12:8-11, 14:13-19). By searching Patel's Gmail account, the means of Popoviz's search exceeded the need and it was not reasonably related in scope to the objectives of the search.

B. Popoviz's search of Patel's iPad and Gmail account was excessively intrusive because Patel's significant expectation of privacy would lead a reasonable employer to expect that a search would reveal personal details about his life.

If an employee's expectation of privacy in a piece of property is significant, a search of that property is excessively intrusive if it is likely to reveal intimate details of his life. See Quon, 560 U.S. at 762. In Quon, the Court found that a search of a government employee's employer-provided pager was reasonable. Id. at 765. When the company distributed the pagers, it provided employees with a policy expressly stating that they "should have no expectation of privacy or confidentiality when using [the pagers]." Id. at 751. While the Court did not make a finding regarding plaintiff's expectation of privacy, it noted that even assuming the plaintiff's expectation of privacy was reasonable, it would have been limited. Id. at 762. The plaintiff could have anticipated that his employer would need access to the pager. Id. The Court held that because the plaintiff's expectation of privacy would have been limited, the search was unlikely to violate his privacy and not excessively intrusive. Id. at 762-63. Relevant here, the Court suggested that the outcome might have been different if the search was of a personal email account:

> [The] audit of messages on [plaintiff's] employer-provided pager was *not nearly as intrusive as a search of his personal email account* . . . would have been. That the search did reveal intimate details of [plaintiff's] life does not make it unreasonable, for under the circumstances a reasonable employer would not expect that such a review would intrude on such matters.

Id. at 762-63 (emphasis added).

Popoviz's search was excessively intrusive because Patel's significant expectation of privacy in his personal iPad and Gmail account made a search likely to violate his privacy and reveal intimate details about his life. Unlike the plaintiff in Quon, whose pager was employer-issued, Patel purchased the iPad himself. (Patel Dep. 11:5-7). Also unlike the plaintiff in Quon, who was provided with a policy granting his employer express permission to audit his messages, Patel received a policy that granted only the IT department access to his iPad and in very limited circumstances – which did not include conducting a search of his personal email account. (CDSS IT Policies). While the plaintiff in Quon had, at best, a limited expectation of privacy, Patel's expectation of privacy was significant. (Patel Dep. 12:5-8). Patel therefore kept private information on his iPad and in his Gmail account that a search was likely to uncover (Patel Dep. 12:5-8). Popoviz's search was excessively intrusive because Patel had a significant expectation of privacy and a reasonable employer would expect a search of his iPad and Gmail account to reveal private information.

C. Because feasible and less intrusive investigatory measures were available to Popoviz and not used, Popoviz's search was excessively intrusive.

A search is unreasonable in scope if less intrusive measures were readily available and not utilized. See Schowengerdt, 823 F.2d at 1336. It is not necessary that the search be the least intrusive method of achieving the desired objectives of the search. Quon, 560 U.S. at 763. However, "if less intrusive methods were feasible, or if the depth of the inquiry or extent of the seizure exceeded that necessary for the government's legitimate purpose," the search is unreasonable and the employee's Fourth Amendment rights are violated. Schowengerdt, 823 F.2d at 1336.

Popoviz's search of Patel's personal email account was excessively intrusive because there were other, less intrusive means of achieving the objectives of the search. Popoviz learned

the information that motivated the search in March 2020. (Popoviz Dep. 6:19-22). He did nothing for three months. (Popoviz Dep. 7:22-8:3). Rather than devising another, less intrusive plan, Popoviz waited three months and then searched Patel's personal Gmail account immediately after learning it was unprotected and in the custody of the IT department. (Popoviz Dep. 10:1-8, 11:6-17). Even the day of the search, Popoviz could have asked Patel about the information, which would have been feasible since Popoviz saw Patel "several times" that day. (Popoviz Dep. 10:9-18). Popoviz's decision to search Patel's personal iPad rather than use the less intrusive methods available to him rendered the search excessively intrusive.

CONCLUSION

Popoviz is not entitled to judgment as a matter of law. A reasonable jury could find that Patel had a legitimate expectation of privacy and Popoviz violated his privacy by conducting an excessively intrusive search that was not reasonably related in scope to the objectives of the search. The record establishes that Patel manifested a subjective expectation of privacy. That expectation was one that society would recognize as reasonable because Patel exercised exclusive control over his iPad, kept personal information on it, and was not subjected to a policy granting CDSS access to his iPad or Gmail account beyond routine software updates. Because of the pervasiveness of electronic devices, society also expects individuals to have privacy in their electronic devices as a general matter. Furthermore, a reasonable jury could conclude that Popoviz's search was unreasonable because it exceeded his right to access Patel's electronic devices under CDSS's IT policies, was likely to reveal personal details of Patel's life, and was far more intrusive than other available options. Popoviz has failed to meet his burden of establishing that he is entitled to judgment as a matter of law. Accordingly, summary judgment must be denied.

DATED: February 26, 2021

Respectfully Submitted
Duncan, Gowen, & Firoz LLP

_____

Meeghan Dooley
501 Market Street
Riverside, CA 92501
(951) 555-5000

ATTORNEYS FOR PLAINTIFF,
PRAVEEN PATEL

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 the Defendant at the following address:

Fried, Pierce & Simon, LLP
1375 East 9th Street
Riverside, CA 92501
Attorney for Defendant

/s/ Meeghan Dooley
Dated: February 26, 2021