IN THE UNITED STATES DISTRICT COURT
DISTRICT COURT OF COLORADO

Civil Action No. 23-cv-01951-CNS

JAQUELINE ARMENDARIZ and CHINOOK CENTER,

Plaintiffs,

v.

CITY OF COLORADO SPRINGS;

DANIEL SUMMEY, a detective with the Colorado Springs Police Department, in his individual capacity;

B.K. STECKLER, a detective with the Colorado Springs Police Department, in his individual capacity;

JASON S. OTERO, a sergeant with the Colorado Springs Police Department, in his individual capacity;

ROY A. DITZLER, a police officer with the Colorado Springs Police Department, in his individual capacity; and

FEDERAL BUREAU OF INVESTIGATION;

Defendants.

PLAINTIFFS' COMBINED RESPONSE IN OPPOSITION TO MOTION TO DISMISS BY THE FEDERAL DEFENDANTS AND DITZLER'S MOTION TO DISMISS AND JOINDER

Table of Contents

Plaintiffs Armendariz and Chinook Center respond to "Motion to Dismiss by the Federal Defendants" (Doc. 49, filed 11/20/23) and "Ditzler's Motion to Dismiss and Joinder in Summey's/United States' Motion to Dismiss" (Doc. 50, filed 11/20/23).

INTRODUCTION

On July 31, 2021, Jacqueline Armendariz was among several activists who participated in a march to bring awareness to the housing crisis in Colorado Springs. Also at the march were Colorado Springs Police Department (CSPD) officers with photos of activists they had been surveilling and hoped to arrest. CSPD officers eventually arrested Shaun Walls and Jon Christiansen, leaders of the non-profit progressive activist organization, the Chinook Center. Armendariz saw police tackling Walls as she was walking her bicycle in the march. She dropped her bicycle when an officer in riot gear ran towards her. The officer, untouched by the bicycle, continued towards the protesters.

After the protest, Defendant Summey, a detective and Task Force Officer at CSPD, reviewed CSPD officers' body camera footage and CSPD drone footage to identify Armendariz as the person who dropped her bicycle at the march. Summey also drafted warrant applications (1) to arrest Armendariz for allegedly attempting to assault an officer and (2) to search her home and seize her digital devices. The search warrant itself does not name any crimes. The supporting affidavit references the alleged attempted bicycle assault, but provides no indicia of probable cause to believe that Armendariz's devices would contain evidence of that crime. Instead, it goes to great lengths to detail Armendariz's political beliefs and associations, and repeatedly equates First Amendment-protected activities with criminality. In applying for the warrant, Summey was supervised by his CSPD supervisor, Roy A. Ditzler, who signed off on the warrant and affidavit.

After CSPD obtained and executed the first search warrant, seizing six of Armendariz's

digital devices, Summey drafted, and Ditzler approved, an application to search each of the seized devices for words like "cop," "protest," and "Walls," unconstrained by any temporal limitation. The warrant they obtained also authorized the seizure of nearly all categories of data that could be found on a device for a period of more than two months. The only theoretical constraint on this seizure was that the data must be "determined to be relevant to this investigation." But the warrant fails to specify what "this investigation" entails, and the affidavit suggests it spans everything from investigating the messages conveyed by protesters' flags to identifying other activists' social media posts expressing anti-police brutality sentiments.

Because the search warrants authorized a sweeping search and seizure of Armendariz's First Amendment-protected activities, they are subject to a heightened Fourth Amendment standard. And because the warrants were so lacking in indicia of probable cause and insufficiently particular that no reasonable officer could rely on them, Defendants violated Armendariz's clearly established Fourth Amendment rights, and they are not entitled to qualified immunity. The warrants likewise violated the Colorado Constitution, and because Plaintiff sued under Colorado's Enhance Law Enforcement Integrity Act, qualified immunity is no defense.

Additionally, Defendants continue to infringe upon Armendariz's rights by retaining copies of her digital data. Armendariz is entitled to injunctive relief ordering Defendants to return or delete copies of her devices and the files extracted therefrom. Defendants moved to dismiss this injunctive relief claim without offering any justification for the continued retention of Armendariz's data, arguing that the Fourth Amendment places no limitations on the government's retention of private data—whether it was obtained lawfully or not. Their position would render constitutional protections theoretical and privacy obsolete.

Defendants also assert that Summey cannot be sued under Section 1983 because his

position as a Task Force Officer automatically made him a federal employee acting under color of federal law. They fail to explain why a CSPD officer supervised by his CSPD supervisor applying to a state court for warrants related to a CSPD-initiated and CSPD-supervised investigation into an alleged state crime cannot be held liable as a CSPD employee acting under color of state law.

For the reasons set forth herein, Plaintiffs respectfully request that the Court deny the Defendants' motions to dismiss.

LEGAL STANDARD

When reviewing a motion to dismiss under Fed. R. Civ. P. 12(b)(6), the court "accept[s] as true all well-pleaded factual allegations in the complaint and view[s] them in the light most favorable to the plaintiff." *Burnett v. Mortg. Elec. Registration Sys., Inc.*, 706 F.3d 1231, 1235 (10th Cir. 2013). A court should not dismiss a claim under Rule 12(b)(6) if "the specific allegations in the complaint '*plausibly support* a legal claim for relief.'" *Choate v. Lemmings*, 294 F. App'x 386, 391 (10th Cir. 2008) (quoting *Alvarado v. KOB–TV, L.L.C.*, 493 F.3d 1210, 1215 n. 2 (10th Cir.2007)). A claim has facial plausibility when the plaintiff pleads "facts supporting all the elements necessary to establish an entitlement to relief under the legal theory proposed." *Forest Guardians v. Forsgren*, 478 F.3d 1149, 1160 (10th Cir. 2007).[1]

Additionally, "[a]sserting a qualified immunity defense via a Rule 12(b)(6) motion . . . subjects the defendant to a more challenging standard of review than would apply on summary judgment." *Hemry v. Ross*, 62 F.4th 1248, 1253 (10th Cir. 2023) (quoting *Thomas v. Kaven*, 765 F.3d 1183, 1194 (10th Cir. 2014)). "In the context of qualified immunity, [the court] may not

[1] To the extent the United States has also moved to dismiss under Fed. R. Civ. P. 12(b)(1) in the context of its FTCA arguments, an FTCA claim should survive unless "the alleged offending conduct" is of the type that the FTCA "shield[s] from suit." *Martin v. United States*, No. 21-CV-02107-MDB, 2023 WL 2743279, at *6 (D. Colo. Mar. 31, 2023).

dismiss a complaint for failure to state a claim unless it appears beyond doubt that plaintiffs cannot prove a set of facts that would entitle them to relief." *Big Cats of Serenity Springs, Inc. v. Rhodes*, 843 F.3d 853, 858 (10th Cir. 2016).

ARGUMENT

I. Claim 1 States a Viable Claim for Relief Because Defendant Summey is Subject to Suit Under Section 1983.

"To state a claim under Section 1983, a plaintiff must allege the violation of a right secured by the Constitution and laws of the United States, and must show that the alleged deprivation was committed by a person acting under color of state law." *West v. Atkins*, 487 U.S. 42, 48 (1988). Armendariz has alleged violations of the First and Fourth Amendments to the U.S. Constitution by CSPD officers Summey and Ditzler, as well as the City of Colorado Springs.

Summey argues that the Section 1983 claim against him must be construed as a *Bivens* claim because, as a "Task Force Officer," he was acting under color of federal law. (Motion to Dismiss by the Federal Defendants ("Fed. MTD"), Doc. 49, at 4.) The facts and law belie this argument.

Federal courts "treat[] local officers assigned to federal task forces as acting *either* under color of state law *or* color of federal law." *Fernandes v. City of Broken Arrow*, No. 16-CV-0630-CVE-FHM, 2017 WL 471561, at *3 (N.D. Okla. Feb. 3, 2017). Courts have "generally held that whether an official acts under color of state or federal law largely depends upon the authority under which the action that causes the constitutional harm is taken." *Jarno v. Lewis*, 256 F. Supp. 2d 499, 503 (E.D. Va. 2003). In answering "difficult" questions about whether action was taken under color of state or federal law in the context of agencies "with both federal and state characteristics," "[a] crucial inquiry is 'whether day-to-day operations are supervised by the Federal [or state]

government.'" *Johnson v. Orr*, 780 F.2d 386, 390 (3d Cir. 1986) (quoting *Detore v. Local 245 Jersey City Public Employers Union*, 615 F.2d 980, 983 (3d Cir.1980)).

In drafting and submitting the warrant applications at issue here, Summey was supervised by Roy A. Ditzler, his CSPD supervisor. (First Amended Complaint, Doc. 12 ("FAC"), ¶ 114.)[2] No defendants have argued that Ditzler had any involvement with the Joint Terrorism Task Force. Ditzler initialed Summey's affidavits as Summey's supervisor and provided his CSPD badge number. (*Id.* ¶¶ 15.) Both warrants indicate that the "Agency" for whom they were submitted was the Colorado Springs Police Department. (*Id.* ¶ 111.) There is no indication that the FBI was exercising supervisory authority over Summey during the events that gave rise to Armendariz's claims against him.

Additionally, CSPD—not the FBI—initiated the criminal case against Armendariz, which was the purported basis for the search warrants. (*Id.* ¶¶ 116–17.) The footage that Summey reviewed to determine who committed the alleged crime of dropping a bicycle came from CSPD body cameras and CSPD drones. (*Id.*, ¶ 57.) Summey checked "local law enforcement databases" to discover CSPD had previously had contact with Armendariz. (Fed. MTD at Ex. 1 (Warrant 1), Doc. 49-1, at 10; Fed. MTD at Ex. 1 (Warrant 1), Doc. 49-2, at 12.) Neither affidavit references any FBI resources or involvement, except that Summey "requests permission for the FBI to be allowed to participate in the search" of Armendariz's residence and devices. (Warrant 1 at 17; Warrant 2 at 28.) The warrants do not request that the FBI lead or supervise the search. The warrants reference no federal crimes, and were issued by a state court. (FAC, ¶ 118.)

[2] Plaintiffs mistakenly referred to Ditzler as Steckler in paragraphs 87 and 113–15 of the Amended Complaint. Defendant Ditzler correctly interpreted those as references Detective Ditzler. Ditzler's (MTD, Doc. 50, at 2 n. 1.)

Moreover, Summey's warrant applications state that he is a police officer for CSPD and has been "so employed for over 6 years." (*Id.* ¶ 112; Warrant 1 at 3; Warrant 2 at 5.) While Defendants highlight the fact that the warrants identify Summey's "Position" as "Task Force Officer," (Fed. MTD at 2), they neglect to mention that this position appears right below "Employed by: Colorado Springs Police Department." (FAC, ¶ 111; Warrant 1 at 2; Warrant 2 at 4.) In other words, Summey's role as a Task Force Officer served CSPD as well as the FBI. (*See also* Warrant 1 at 17 (noting Summey "regularly works joint investigations with CSPD and the FBI"); Warrant 2 at 28 (same).) These facts plausibly support a claim for relief under Section 1983.

Similar facts led Judge Wang to conclude that a CSPD officer was not acting under color of federal law in *Halik v. Brewer*, No. 21-CV-00508-PAB-NYW, 2022 WL 488608 (D. Colo. Feb. 17, 2022), *report and recommendation adopted in part, rejected in part on other grounds*, No. 21-CV-00508-PAB-NYW, 2022 WL 897105 (D. Colo. Mar. 28, 2022). There, a plaintiff sued a CSPD officer assigned to a federal task force and members of the CSPD's SWAT team for constitutional violations arising from an invalid state-issued search warrant. *Id.* at *1. Judge Wang decided there were insufficient allegations to conclude the CSPD officer was acting under color of federal law, because the warrant was obtained by the CSPD, the affiant was identified as a CSPD detective, the warrant affidavit stated it was based on "information provided by officers and/or detectives with the Colorado Springs Police Department," and "[w]hile [the plaintiff] alleges that federal ATF agents 'accompanied' the local SWAT team in their execution of the search warrant, there are no allegations reasonably suggesting that the raid, or any other purported misconduct by law enforcement, was taken either at the behest of federal agents, or in connection with any federal purpose." *Id.* at *6.

Similarly, in a case where there was no evidence that officers of a city police department "were carrying federal credentials, supervised by federal officials, paid by the federal government, or covered by federal benefits," there was insufficient evidence to demonstrate the officers acted under color of federal law. *Pettiford v. City of Greensboro*, 556 F. Supp. 2d 512, 537 (M.D.N.C. 2008).

The only authority Defendants cite for the proposition that Summey was acting under color of federal law is the Sixth Circuit's statement that "the nature and character of a cooperative federal-state program is determined by the source and implementation of authority for the *program*, not for the particular work that the agency chooses, in the exercise of its authority, to perform on a given day." *King v. United States*, 917 F.3d 409, 433 (6th Cir. 2019), *rev'd on other grounds sub nom. Brownback v. King*, 141 S. Ct. 740 (2021). (Fed. MTD at 4 n. 2.) But Defendants do not explain why the authority for the *Joint* Terrorism Task Force's programs in which Summey participated were not plausibly authorized and implemented by CSPD officers acting under color of state law. Indeed, the Sixth Circuit recognized that "[a] defendant's actions performed pursuant to a mixed federal and state program may . . . be actions under color of state law." *Id.* at 432-433. (quoting *Rowe v. Tennessee*, 609 F.2d 259, 266 (6th Cir. 1979) (internal quotations omitted)).

Moreover, the facts here are distinguishable from those in *King*. In *King*, the court held that a plaintiff could not sue a Grand Rapids Police detective under Section 1983 because he was working full time with the FBI task force, and there were no allegations that the state was involved in authorizing or administering the task force. *Id.* Here, on the other hand, Armendariz has alleged facts demonstrating that Summey was acting under color of state law and within the scope of his employment as a CSPD officer while he was assigned to be a Task Force officer, (FAC, ¶¶ 15,

111), and that the CSPD was heavily involved in supervising and administering his work (*id.* ¶¶ 88, 111, 114.) Armendariz has sufficiently pled that Summey was acting under color of state law, and this Court should therefore reject Summey's attempt to recast Plaintiff's 1983 claim as a *Bivens* claim.

II. Even if the Court Were to Interpret Claim 1 As a *Bivens* Claim Against Summey, Dismissal Would Be Improper.

The Fourth Amendment "guarantees to citizens of the United States the absolute right to be free from unreasonable searches and seizures carried out by virtue of federal authority." *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 392, (1971) (quoting *Bell v. Hood*, 327 U.S., at 684). Recognizing that damages remedies are crucial to ensuring meaningful enforcement of constitutional rights, the Supreme Court in *Bivens* "established that the victims of a constitutional violation by a federal agent have a right to recover damages against the official in federal court despite the absence of any statute conferring such a right." *Carlson v. Green*, 446 U.S. 14, 18 (1980).

Specifically, "*Bivens* held that the Fourth Amendment guarantee against 'unreasonable searches and seizures' was a constitutional right which Bivens could enforce through a private cause of action, and that a damages remedy was an appropriate form of redress." *Davis v. Passman*, 442 U.S. 228, 234 (1979); *see also Nat'l Commodity & Barter Ass'n v. Archer*, 31 F.3d 1521, 1527 (10th Cir. 1994) ("[I]f claims of violations of First or Fourth Amendment rights are proven, then a *Bivens* remedy may be afforded to the plaintiffs for recovery of damages for such constitutional wrongs.").

A *Bivens* remedy exists where a case arises in a context not meaningfully different from those in which the Supreme Court has previously implied a damages action. *Ziglar v. Abbasi*, 582 U.S. 120, 139–40 (2017). This case arises in the same context as *Bivens* itself: an unreasonable

search and seizure. Summey argues that this case presents a new context because he obtained warrants, whereas the officers in *Bivens* did not. But courts have upheld *Bivens* actions in contexts where officers relied on a defective warrant, including where there was no excessive force. *See, e.g.*, *Groh v. Ramirez*, 540 U.S. 551 (2004) (*Bivens* action against ATF agent who obtained and executed warrant lacking particularity); *Nat'l Commodity & Barter Ass'n*, 31 F.3d at 1521 (*Bivens* action against IRS officers for obtaining and executing search warrants violating the First and Fourth Amendments). Armendariz has plausibly stated a claim for relief under *Bivens*.

III. Summey and Ditzler Are Not Entitled to Qualified Immunity on Claim 1.

When a defendant claims qualified immunity, a plaintiff must show: "(1) that the defendant's actions violated a constitutional or statutory right, and (2) that the rights alleged to be violated were clearly established at the time of the conduct at issue." *Anderson v. Blake*, 469 F.3d 910, 913 (10th Cir. 2006). Both prongs are met here.

Warrant 2 authorized a keyword search of six digital devices for the words "Police, officer, cop, pig, bike, bicycle, attack, assault, 150th, celebration, protest, housing, human, right, yt, Chinook, Center, Jon, Jonathan, Sam, Samantha, Christiansen, Crustyansen, Chrischeeansen, Shaun, [and] Walls," without any temporal limitation, and without any indication that searching for any of these words would turn up evidence of a particular crime. (Warrant 2 at 29.)

It also authorized the search of Armendariz's devices for "[p]hotos, videos, messages (Whether they be text messages or any application on the phone or computer capable of sending messages) emails, and location data, for the time period of 6/5/2021 through 8/7/2021 that are determined to be relevant to this investigation." (*Id.*) The warrant provided no guidance on how to determine whether data was relevant to the amorphous investigation at issue.

Moreover, neither the warrant to seize Armendariz's devices nor the warrant to search them

was based on probable cause to believe evidence of a crime would be found on each device. The warrants swept up vast amounts of protected speech, failed to comply with the constitutional probable cause and particularity requirements, and violated clearly established law.

A. The Warrants Violated Armendariz's Constitutional rights.

"The [F]ourth [A]mendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a 'general, exploratory rummaging in a person's belongings.'" *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). "A warrant is adequately particularized as to the 'things to be seized' when it allows an executing officer to 'reasonably ascertain and identify the things authorized to be seized,'" *People v. Seymour*, 2023 CO 53, ¶ 50, 536 P.3d 1260, 1276 (quoting *People v. Roccaforte*, 919 P.2d 799, 803 (Colo. 1996)), "with little discretion to decide which records are responsive." *Id.* (citing *Marron v. United States*, 275 U.S. 192, 196 (1927)).

The Fourth Amendment additionally requires "that the scope of the warrant be limited to the specific areas and things for which there is probable cause to search." *United States v. Leary*, 846 F.2d 592, 605 (10th Cir. 1988). Probable cause exists only when there is a "fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). There must be a "nexus . . . between suspected criminal activity and the place to be searched." *United States v. Mora*, 989 F.3d 794, 800 (10th Cir. 2021) (quoting *United States v. Biglow*, 562 F.3d 1272, 1278 (10th Cir. 2009)).

The particularity and probable cause requirements are especially important in the context of digital devices, which "store and intermingle a huge array of one's personal papers in a single place." *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009). Warrants related to the search or seizure of digital devices must "*affirmatively limit* the search to evidence of specific federal

crimes or specific types of material." *Id.*

Additionally, the Fourth Amendment standards are heightened where, as here, "the materials sought to be seized may be protected by the First Amendment." *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978). Judges must remain vigilant to the threat that "unrestricted power of search and seizure" could function as "an instrument for stifling liberty of expression." *Id.* at 564 (quoting *Marcus v. Search Warrant*, 367 U.S. 717, 729 (1961)).

1. The Keyword Search Was Unsupported by Probable Cause and Insufficiently Particular.

Warrant 2 authorized the search for 26 words on each of Armendariz's devices and affirmatively rejected the need for any temporal limitation, stating "these terms would be relevant to the investigation regardless of the time period in which they occurred." (Warrant 2 at 29.) The affidavit provided no indicia of probable cause to believe that data containing words like "celebration" and "officer" would constitute evidence of an attempted assault on July 31, 2021—let alone data from ten years ago. Allowing officers to rummage through devices in this manner recalls the reviled general warrants of the eighteenth century. *See United States v. Zemlyansky*, 945 F. Supp. 2d 438, 460 (S.D.N.Y. 2013) (absence of temporal limitation on search "reinforces the Court's conclusion that the . . . warrant functioned as a general warrant"); *State v. Turay*, 532 P.3d 57, 75-76, (Or. 2023) (in the warrant authorizing search for nine categories of data, some categories were insufficiently particular for failing to specify a time period).

The affidavit provides no reason to believe that a search for "human" or "right" would turn up evidence of a crime. But such a search would certainly capture a wide swath of political speech—commentary on anything from *right*-wing candidates' policy positions to support for a bill related to *human* trafficking—all protected by the First Amendment. *See Sweezy v. New*

Hampshire, 354 U.S. 234, 250 (1957) ("[T]he right to engage in political expression and association" was "enshrined in the First Amendment of the Bill of Rights.").

Similarly, rather than explaining why a keyword search for "Chinook" would turn up evidence of a crime, Summey's affidavit notes that the Chinook Center is "the central hub for multiple activist groups and their members," and that the Chinook Center and protesters were promoting the view that "Housing is a Human Right." (Warrant 2 at 5–6; *see also id.* at 20.) A warrant that allows officers to fish for information about an association promoting a view with which they disagree simply fails to satisfy Fourth Amendment requirements—especially when applied with the "scrupulous exactitude" required here. *See Stanford v. Texas*, 379 U.S. 476, 485 (1965).

The only references to "cop" or "pig" in Summey's affidavit appeared in social media posts by Shaun Walls expressing frustration with police. (Warrant 2 at 22–25.) A different activist's posts expressing his views about the police does not provide probable cause to believe that searching Armendariz's devices for Walls' words would reveal evidence that Armendariz attempted to assault an officer by dropping a bicycle at a protest. But it is certain that a search for these words would reveal a vast amount of Armendariz's speech—including criticism of police officers—protected by the First Amendment. *See City of Houston, Tex. v. Hill*, 482 U.S. 451, 461 (1987); *Jordan v. Jenkins*, 73 F.4th 1162, 1168 (10th Cir. 2023).

The affidavit also provides no explanation for why mentions of Walls or other activists on Armendariz's devices would reveal evidence of the alleged attempted assault. While Summey asserted that Armendariz's appearance on a podcast hosted by Christiansen and Walls "shows her connection to the activist community, and her closeness with Christiansen and Walls," (Warrant 2 at 27), he does not explain how a close relationship with other activists would justify searching

Armendariz's devices for evidence of an alleged attempted bicycle assault she committed alone at the spur of the moment during an overly-aggressive arrest of someone for allegedly jay-walking.

The First Amendment protects "[t]he right to engage in expressive activities anonymously, without government intrusion or observation" as well as the right to speak, associate with others, and receive information and ideas. *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1051–53 (Colo. 2002), *as modified on denial of reh'g* (Apr. 29, 2002). "Anonymity is vital because individuals may be 'chilled' from exercising their rights when expressive activities are publicly disclosed." *Seymour*, 2023 CO 53, ¶ 38, 536 P.3d at 1274 (quoting *Tattered Cover*, 44 P.3d at 1052–53).

The warrants authorized fishing for communications with other activists and mentions of political topics without reason to believe they would reveal evidence of a crime, and thereby ran afoul of the Supreme Court's consistent admonitions against "governmental action . . . denying rights and privileges solely because of a citizen's association with an unpopular organization." *Healy v. James*, 408 U.S. 169, 185–86 (1972). "[G]uilt by association alone, without [establishing] that an individual's association poses the threat feared by the Government,' is an impermissible basis upon which to deny First Amendment rights." *Id.* at 186; *cf. Poolaw v. Marcantel*, 565 F.3d 721, 730, 738 (10th Cir. 2009), *as amended* (July 24, 2009) ("[M]ere propinquity" to someone suspected of a crime is "insufficient to establish probable cause" for a search warrant).

Defendants argue that, because the warrant did not need to contain "search protocols," the keywords "could not have invalidated Warrant 2." (Fed. MTD at 16.) But a warrant's description of an overbroad search cannot be rendered constitutional by referring to the description as "search protocol." Even the most particularized warrant would still be unconstitutional if it particularly described a search for which there was no probable cause. Here, the keyword search is both

insufficiently particular and overbroad. Because the keyword search provision failed to cabin the search to a particular timeframe and authorized a search reaching vast amounts of protected speech without probable cause, it violated the Fourth Amendment.

2. The Requirement that the Data Seized Be "relevant to this investigation" Is Insufficiently Particular.

The warrants authorized the seizure of broad categories of data so long as they were "determined to be relevant to this investigation," without providing any description of "this investigation" or any guidance on determining which data is "relevant" to it. This lack of specificity renders the warrant insufficiently particular. *See United States v. Lofstead*, 574 F. Supp. 3d 831, 844 (D. Nev. 2021) (warrant to search "[a]ny and all records and materials that may be found within [the phone], in any format and media (including, but not limited to; images videos, e-mails, chat logs, text messages, instant messages and electronic messages), pertaining to the Target Offenses" was insufficiently particular and violated the Fourth Amendment).

Far from leaving "nothing . . . to the discretion of the officer executing the warrant," *Voss*, 774 F.2d at 404 (quoting *Stanford*, 379 U.S. at 485-86), the warrants allowed officers unfettered discretion to decide what "this investigation" encompassed, and which data was relevant to it. *See United States v. Hillyard*, 677 F.2d 1336, 1339 (9th Cir. 1982) (describing as "unlawfully general" searches "where the accompanying warrant 'left to the executing officers,' rather than to the magistrate upon issuance, 'the task of determining what items fell within broad categories stated in the warrant' and where there were no clear guidelines distinguishing between property which was contraband and that which was not" (quoting United *States v. Drebin*, 557 F.2d 1316, 1322-23 (9th Cir. 1977))); *Taylor v. State*, 260 A.3d 602, 616 (Del. 2021) (warrant allowing investigators to search smartphone for "any and all data" "pertinent to the criminal investigation" was "unlimited in scope" and constituted an unlawful general warrant).

Voss v. Bergsgaard is instructive. 774 F.2d 402. There, IRS agents had probable cause to believe the National Commodities and Barter Association (NCBA) was engaged in fraud and obtained warrants for the seizure of many types of records, including "books, literature and tapes advocating nonpayment of federal income taxes; publications of tax protestor organizations; and literature relating to communications between persons conspiring to defraud the IRS." *Id.* at 404. While the warrant stated that all types of evidence listed "are evidence of violations of Title 18, United States Code, Section 371," the reference to the conspiracy statute was not "a constitutionally adequate particularization of the items to be seized," because the statute is broad and "places no real limitation on the warrant." *Id.* at 405. Similarly, Warrant 2's reference to "this investigation"—which is not tied to any crime in the warrant itself—does not limit the executing officers' discretion to "rummag[e] through a person's belongings, in search of evidence of even previously unsuspected crimes or of no crime at all." *Id.* at 405. Additionally, as in *Voss*, "[t]he warrants' overbreadth is made even more egregious by the fact that the search at issue implicated free speech and associational rights." *Id.* The warrant here authorized the seizure of any messages or emails to, from, or about political organizers and political topics. Here, as in *Voss*, there was "no justification for seizing records and documents relating to [the target's] legitimate activities." *Id.* at 406.

Defendants rely on information in the affidavit to argue that the warrant itself was sufficiently particular. (Fed. MTD at 9, 11.) But nothing in the affidavit limits the bounds of "this investigation." To the contrary, the affidavit recounts a sprawling expedition into everything from Armendariz's feelings about white people (based on Summey's use of a slang dictionary to look up the term "yt supremacy"), (Warrant 2 at 16), to how "active politically" Armendariz is, (*id.* at 16, 18).

The Ninth Circuit rejected a claim that an affidavit offered "the level of guidance necessary to cure a facially invalid warrant" in *United States v. Kow*, 58 F.3d 423, 429 (9th Cir. 1995). The *Kow* warrant authorized the seizure of fourteen categories of business records but "contained no limitations on which documents within each category could be seized or suggested how they related to specific criminal activity." *Id.* at 427. The court determined that, "[a]lthough the affidavit contained some information that could have been used to make the warrant more specific . . . , the information was buried among thirty-five pages of less helpful material and would not have assisted officers executing the warrant to narrow the scope of their search." *Id.* at 430.

Summey's affidavit, too, is 23 pages long and contains information entirely irrelevant to any alleged crime. The affidavit contains Summey's Internet research supposedly indicating that red flags symbolize socialism and communism. (Warrant 2 at 6.) It also contains Summey's assessment of Armendariz's LinkedIn profile, which "shows she is active politically in Colorado Springs and Pueblo." (Warrant 2 at 16.) And a key feature of "this investigation" appears to be treating protest activity as "illegal." (*See, e.g.*, Warrant 2 at 5, 19, 25, 26, 27.) If the scope of "this investigation" is determined by the affidavit, then it appears to be even more wide-ranging than the warrant on its own, causing its own additional constitutional infirmities.

While the fourteenth page of the affidavit includes one mention of a specific crime—attempted assault—the affidavit as a whole suggests Defendants' view of "this investigation" was much broader than simply locating evidence that Armendariz dropped her bicycle in front of an officer at the July 31 housing rights march. And no officer executing the warrant would have known where their discretion ended.

3. There Was No Probable Cause to Seize or Search All of Armendariz's Devices.

In support of the application for the warrant to seize all "Digital media storage devices, to

include phones, computers, tablets, thumb drives, and external hard drives found to be associated with Jacqueline Armendariz," (Warrant 1 at 18), Summey made no attempt to link any of Armendariz's devices with the alleged crime, aside from boilerplate statements about the use of digital devices generally. The affidavit states: "[P]eople who engage in illegal protest activity frequently carry their phones with them to take photos of their activity and message others who are also participating in illegal protest activity." (Warrant 1 at 17.)

But general assertions that people who commit certain types of crimes often use their cell phones in the process, and boilerplate language about the types of data that may be found on cell phones, are insufficient to establish probable cause to search a particular cell phone—let alone every digital media storage device. *See Mora*, 989 F.3d at 801 ("The affiant stated . . . that alien smugglers often use electronic communication devices, GPS devices, and electronic banking systems to conduct operations and store records. None of those boilerplate statements, however, are specific to Defendant's crime or circumstances."); *United States v. Ramirez*, 180 F. Supp. 3d 491, 494, 495 (W.D. Ky. 2016) (insufficient information to establish probable cause to search defendant's phone where defendant possessed phone at time of his arrest, affiant noted "that individuals may keep text messages or other electronic information stored in their cell phones which may relate them to the crime and/or co-defendants/victim," and "cell phones . . . are generally considered the 'tools of the trade' of drug traffickers."); *United States v. Oglesby*, No. 4:18-CR-0626, 2019 WL 1877228, at *4–5 (S.D. Tex. Apr. 26, 2019) (generalizations about how cell phones are used and beliefs about evidence they might contain were insufficient to establish a nexus between the alleged crime and the suspect's phone).

In the modern era, cell phones are "a pervasive and insistent part of daily life," creating and storing "a cache of sensitive personal information" as a person moves about the world. *Riley*

v. California, 573 U.S. 373, 385, 395 (2014). Location information alone provides "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (quoting *United States v. Jones*, 565 U.S. 400, 415, (2012) (Sotomayor, J., concurring)). Combined with all the other data on cell phones, these devices might contain evidence of nearly everything a person does.

But if these observations were sufficient to establish probable cause to search a person's cell phone without any specific facts linking a particular device to the alleged criminal activity, then police could seize and search cell phones in every case, warrants would merely be formalities, and the Fourth Amendment's protections would be eviscerated. *See Oglesby*, 2019 WL 1877228, at *6 (While "a person's cell phone contains evidence of almost any activity in which they participate," "[i]f these statements are held sufficient [to establish the nexus required for probable cause], every accusation of criminal activity would automatically authorize a search of the suspect's cell phone, transforming every arrest warrant into a search warrant and directly contravening the Supreme Court's decision in *Riley*."); *Commonwealth v. White*, 475 Mass. 583, 591, 59 N.E.3d 369, 377 (Mass. 2016) (If it were true that "there exists a nexus between a suspect's criminal acts and his or her cellular telephone whenever there is probable cause that the suspect was involved in an offense, accompanied by an officer's averment that, given the type of crime under investigation, the device likely would contain evidence," then "it would be a rare case where probable cause to charge someone with a crime would not open the person's cellular telephone to seizure and subsequent search.").

And if the assertion that "people store digital data on numerous devices" were enough to establish probable cause to seize all devices (Warrant 1 at 15), there would similarly be probable

cause to search all of a suspect's devices in nearly every investigation. *Cf. Voss*, 774 F.2d at 406 (no probable cause to seize nearly all of organization's business records without "probable cause to believe that fraud pervaded every aspect" of the organization); *State v. Castagnola*, 46 N.E.3d 638, 654 (Ohio 2015) ("[W]e are not inclined to leap to the conclusion that the information stored on a phone will necessarily be backed up on a computer"). Without a specific nexus between each of Armendariz's devices and the alleged attempted assault, there was no probable cause to seize each device.

After six of Armendariz's devices were seized, Warrant 2 authorized a similarly overbroad search of each device. Far from establishing a "nexus . . . between suspected criminal activity and the place to be searched," *Mora*, 989 F.3d at 800, the affidavit in support of Warrant 2 contained information suggesting that some of the devices were particularly *unlikely* to contain data relevant to the alleged attempted assault.

One of the computers searched pursuant to Warrant 2 had stickers on it "denoting it is a work computer, and is property of US Senator Michael Bennet's Office, and is US Senate Property." (Warrant 2 at 19.) Summey articulated no reason to believe that evidence of Armendariz dropping her bike at a Saturday protest would be found on her work computer, aside from his claimed "training and experience" that "people often engage in personal communications with their work devices even though it is oftentimes not allowed by company policy."[3] If this statement

[3] Defendants argue the fact that Armendariz's supervisor told Summey that Armendariz "attended the protest" and "sent her digital media of the protest" provides cause to believe "Plaintiff's devices possessed evidence that would be relevant to her prosecution." (Fed. MTD at 13.) But Armendariz's work computer was seized before Summey spoke with Armendariz's supervisor. And in any case, Summey's statement cannot justify the search of six different devices for a vast array of information besides "digital media of the protest" such as emails and location information.

were sufficient to provide probable cause here, then there would *always* be probable cause to search a person's work devices for evidence of non-work-related crimes.

Additionally, Warrant 2 authorized the seizure of data from a period of more than two months, even though Summey reviewed bodycam footage of the incident, and therefore knew the exact moment it occurred. (Warrant 2 at 7 (discussing photos from Officer Gilmore's bodycam from "the moment the suspect attempted to assault Officer Spicuglia").) Instead of seeking a warrant to obtain Armendariz's location information *at the time of the alleged bike-dropping crime*, Defendants impermissibly sought location data for the entire summer. *See United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) (holding overbroad a warrant that authorized a search for records from a six-year period when the evidence in support of probable cause all came from a three-month period); *Burns v. United States*, 235 A.3d 758, 773 (D.C. 2020) ("To be compliant with the Fourth Amendment, the warrant must specify the particular items of evidence to be searched for and seized from the phone and be strictly limited to the time period and information or other data for which probable cause has been properly established.").

Defendant Ditzler contends that the lengthy time period was justified by Summey's statement that it "would allow for any planning leading up to the crime, the period when the crime took place, and the subsequent taking of credit for committing a violent act against a police officer." (Ditzler MTD at 4; Warrant 2 at 29.) But the affidavit includes no facts to suggest that Armendariz planned to drop her bike at the protest or subsequently took credit for doing so—let alone that any such planning or credit would be in the form of photos, location data, etc.

Moreover, a search warrant must not only satisfy the probable cause and particularity requirements; it must also meet the "overriding test" of reasonableness. *See Zurcher*, 436 U.S. at 559–60; *United States v. Koyomejian*, 970 F.2d 536, 550 (9th Cir. 1992) (Kozinski, J., concurring).

The constitutional command that searches be "reasonable" requires that "when the State seeks to intrude upon an area in which our society recognizes a significantly heightened privacy interest, a more substantial justification is required to make the search 'reasonable.'" *Winston v. Lee*, 470 U.S. 753, 767 (1985); *see Doe v. Bagan*, 41 F.3d 571, 576 (10th Cir. 1994). This means that "even where the government shows probable cause, describes the scope of the search with particularity and complies with every other procedural requirement for issuance of a warrant, the court still must inquire into the 'extent of the intrusion on [the individual's] privacy interests and on the State's need for the evidence.'" *Koyomejian*, 970 F.2d at 550 (Kozinski, J., concurring) (quoting *Winston*, 470 U.S. at 763).

Here, the only specific crime identified in the affidavit is the alleged attempted assault of a police officer by dropping a bicycle in front of him. The affidavit shows that police already had overwhelming evidence, based on photos from the march, that Armendariz was the person they were looking for. (*See* Warrant 1 at 5–10.) The government's need for additional evidence was not so great as to justify the tremendous intrusion of a search of cellphones, computers, and external hard drives. Indeed, the scope of the intrusion provides strong evidence of Defendants' retaliatory motives.

B. Armendariz's Constitutional Rights Were Clearly Established.

"A plaintiff can demonstrate that a constitutional right is clearly established by reference to cases from the Supreme Court, the Tenth Circuit, or the weight of authority from other circuits. There need not be precise factual correspondence between earlier cases and the case at hand, because general statements of the law are not inherently incapable of giving fair and clear warning." *Mink v. Knox*, 613 F.3d 995, 1001 (10th Cir. 2010) (quoting *Archuleta v. Wagner*, 523

F.3d 1278, 1283 (10th Cir. 2008)). Armendariz's right to be free from unreasonable searches and seizures was clearly established when Defendants prepared and obtained the warrants at issue.

"The uniformly applied rule is that a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional." *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n.5 (1984) (citing numerous cases). Defendants are not entitled to qualified immunity for obvious violations of the particularity requirement, because "[g]iven that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid." *Groh*, 540 U.S. at 563; *Cassady v. Goering*, 567 F.3d 628, 644 (10th Cir. 2009).

In *United States v. Leary*, the Tenth Circuit considered a warrant directing the executing officer to seize records "relating to" violations of federal export laws. *Leary*, 846 F.2d at 609. The court held that "[a] reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized," and the warrant at issue instead left officers "to their own discretion." *Id.* The warrant was thus "so facially deficient in its description of the items to be seized that the executing officers could not reasonably rely on it." *Id.* Here, too, Defendants relied on a facially deficient warrant that allowed officers to seize any pictures, videos, messages, etc. that they deemed "relevant" to an undefined "investigation."

Additionally, it has long been clearly established that the scope of a warrant must not exceed the probable cause to support it. *See id.* at 605 ("a search warrant is . . . impermissibly overbroad if it authorizes the search and seizure of evidence that is not supported by probable cause"); 4 W. LaFave, *Search and Seizure* § 11.3(d) (2d ed. 1987) ("An otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based."). It is also "well-settled that for probable cause

to exist there must be a 'nexus between . . . suspected criminal activity and the place to be searched.'" *United States v. Gonzales*, 399 F.3d 1225, 1228 (10th Cir. 2005).

Here, the affidavit made no attempt to demonstrate probable cause to believe that a search for the keywords would turn up evidence of the alleged crime. And beyond boilerplate assertions about the way people use digital devices, the affidavit made no attempt to establish a nexus between the alleged attempted assault of an officer with a bicycle and each of Armendariz's digital devices. Instead, the warrants authorized sweeping, overbroad searches of nearly all data on all of Armendariz's digital devices. Where a warrant is "impermissibly overbroad, the clearly established prong is easily satisfied." *Cassady*, 567 F.3d at 643. Moreover, no reasonable officer would believe that a warrant was constitutionally authorized where the affidavits harped on the target's political activism and associations instead of providing facts to establish probable cause. S*ee Jordan*, 73 F.4th at 1171 ("[I]t is clearly established that 'a government official may not base her probable cause determination on . . . speech protected by the First Amendment.'" (quoting *Mink*, 613 F.3d at 1003–04)).

Ditzler argues he is entitled to qualified immunity because "it was not clearly established in August 2021 that merely reviewing and approving a search warrant affidavit could give rise to a First Amendment retaliation claim or that the search warrant for Armendariz's digital devices violated clearly established law." (Ditzler MTD at 8.) But "an officer need not execute a search personally to be liable." *Poolaw*, 565 F.3d at 732. By approving the warrant application and affidavit, Ditzler caused a deprivation of Armendariz's clearly established rights. *See id.* at 732–33; *Cassady*, 567 F.3d at 644 (denying qualified immunity to an officer whose subordinate obtained an unconstitutional warrant).

Defendants make much of the fact that the warrants were approved by judges. (Fed. MTD at 18; Ditzler MTD at 2.) But officers are not automatically entitled to qualified immunity "simply because a magistrate had approved the [warrant] application." *Messerschmidt v. Millender*, 565 U.S. 535, 554 (2012); *see also People v. Leftwich*, 869 P.2d 1260, 1269 n. 11 (Colo. 1994) ("[T]he question of reasonableness is to be judged as of the time of warrant application and thus without consideration of the fact that the magistrate thereafter issued a warrant."). An officer cannot escape liability by "rely[ing] on the judgment of a judicial officer in finding that probable cause exists," because the relevant inquiry is "whether a reasonably well-trained officer in [the officer's] position would have known that his affidavit failed to establish probable cause and that he should not have applied for the warrant." *Malley v. Briggs*, 475 U.S. 335, 345 (1986). Moreover, because Summey "himself prepared the invalid warrant, he may not argue that he reasonably relied on the Magistrate's assurance that the warrant contained an adequate description of the things to be seized and was therefore valid." *Groh*, 540 U.S. at 564. In other words, it is incumbent on Defendants to adhere to clearly established Fourth Amendment requirements, and they cannot evade liability by blaming another for their own errors which any reasonable officer would have caught. Here, Defendants plainly violated clearly established constitutional requirements and must be held liable.

IV. The FBI Continues to Violate Armendariz's Rights By Unlawfully Retaining Her Digital Data.

Armendariz has a significant interest in keeping her digital data private. *See Church of Scientology of California v. United States*, 506 U.S. 9, 13 (1992) ("A person's interest in maintaining the privacy of her 'papers and effects' is of sufficient importance to merit constitutional protection."). By retaining Armendariz's illegally obtained data, Defendants continue to violate her constitutional rights. *See Lindell v. United States*, 82 F.4th 614, 622 (8th Cir. 2023) ("The retention of data unrelated to the government's investigation and which goes

beyond the terms of the search warrant implicates an individual's right to be free from unreasonable searches and seizures.").

Courts have long recognized that the government's continued retention of information injures the owner, and that the return or destruction of that information is a viable remedy. *See, e.g.*, *Doe v. U.S. Air Force*, 812 F.2d 738, 740-41 (D.C. Cir. 1987) (appropriate relief includes the government's surrender of retained copies and information obtained by an unreasonable search and seizure); *ADAPT of Phila. v. Phila. Hous. Auth.*, 417 F.3d 390, 393-94 (3rd Cir. 2005) (finding "return or destruction" of compilations made from confidential information would "alleviate, at least in part, any affront to the privacy rights of the individuals"); *Reich v. Nat'l Eng'g. Contracting. Co.*, 13 F.3d 93, 98 (4th Cir. 1993) (In challenge to collection of confidential information by the Occupational Safety and Health Administration, court found that the "privacy interest . . . in the delivered copies . . . plainly would be benefited by an order requiring OSHA to return or destroy these copies").

The Eighth Circuit recently recognized that "absent sufficient justification, the government has no right to hold onto property that is not contraband indefinitely." *Lindell*, 82 F.4th at 621. *Lindell* concerned the FBI's investigation into a security breach involving the publishing of forensic images of election software used in the 2020 election in Mesa County. *Id.* at 617. As part of the investigation, the FBI obtained a warrant to seize and search the cellphone of Mike Lindell, the CEO of MyPillow who had been vocal about advancing his theories of election fraud. *Id.* Lindell maintained access to "the vast majority of information contained on the cell phone" because it had been backed up shortly before the seizure. *Id.* at 620. But even so, the Eighth Circuit held that, "[g]iven the necessity of cell phones in everyday life and the related privacy concerns regarding the breadth of data that they contain, the government's continued retention of Lindell's

cell phone and all its data (including that which is entirely unrelated to the government's investigation), without adequate justification, could amount to a callous disregard of Lindell's constitutional rights." *Id.* at 622.

Contrary to Defendants' contentions here, (Fed. MTD at 21), "[t]he government's continued retention of the phone and all its data raises constitutional issues distinct from the lawfulness of the search warrant or its execution." *Lindell*, 82 F.4th at 621. Regardless of whether the warrants for the seizure and search of Armendariz's devices were lawful, the government has put forth no justification for continuing to retain the data, and therefore, its continued retention is unlawful.

Many of the cases Defendants cite in support of their position do not concern the unique privacy concerns presented by the retention of vast amounts of personal, private digital data. *See Conyers v. City of Chicago*, 10 F.4th 704, 706 (7th Cir. 2021) (class action challenging city's policy of selling or destroying arrested persons' seized property it if it is unclaimed after 30 days); *Case v. Eslinger*, 555 F.3d 1317, 1330 (11th Cir. 2009) (challenge to officers' disposal of personal property, including tractor, tire rims, money, and credit cards); *Winters v. Bd. of Cnty. Comm'rs*, 4 F.3d 848, 856 (10th Cir. 1993) (concerning improper disposition of a seized ring); *Snider v. Lincoln Cnty. Bd. of Cnty. Comm'rs*, 313 F. App'x 85, 88, 93 (10th Cir. 2008) (retention of seized firearms); *Denault v. Ahern*, 857 F.3d 76, 79 (1st Cir. 2017) (retention of car and possessions inside).

Defendants also cite *Malik v. U.S. Department of Homeland Security*, which involved the seizure and search of an immigration attorney's phone when he was returning from international travel, but the court there relied on Fifth Circuit precedent treating Fourth Amendment protections

as "lessened by the tradition of inspection procedures at the border." 78 F.4th 191, 194, 200 (5th Cir. 2023) (quoting *United States v. Molina-Isidoro*, 884 F.3d 287, 291 (5th Cir. 2018)).

Finally, Defendants cite *Matter of the Search of Twenty-Six Digital Devices*, in which the District Court for the District of Columbia held that, when evaluating a warrant application to search data already within the government's possession, the court need not conduct "an additional and freestanding reasonable analysis" to determine whether the government's possession of that data had been reasonable. No. 21-SW-233 (GMH), 2022 WL 998896, at *6 (D.D.C. Mar. 14, 2022). But here, Armendariz is directly challenging the current, unjustified, continued retention of her data.

Other courts have recognized that the Fourth Amendment "is implicated by a delay in returning . . . property, whether the property was seized for a criminal investigation, to protect the public, or to punish the individual." *Brewster v. Beck*, 859 F.3d 1194, 1197 (9th Cir. 2017) (quoting *Sandoval* v. *County of Sonoma*, 72 F.Supp.3d 997, 1004 (N.D. Cal. 2014)); *United States v. Place*, 462 U.S. 696, 709 (1983); *Lindell*, 82 F.4th at 622. "A seizure is justified under the Fourth Amendment only to the extent that the government's justification holds force. Thereafter, the government must cease the seizure or secure a new justification." *Brewster*, 859 F.3d at 1197. In *United States v. Place*, law enforcement seized Place's luggage, suspicious that there might be narcotics in it. 462 U.S. 696, 699 (1983). "But it wasn't this initial seizure that concerned the Supreme Court. Rather, it was the '90-minute detention of [Place's] luggage [that was] sufficient to render the seizure unreasonable.'" *Brewster*, 859 F.3d at 1197 (quoting *Place*, 462 U.S. at 710).

The government's interest in retaining the data from Armendariz's devices must be balanced against Armendariz's interest in their giving it back or destroying it. *Lindell*, 82 F.4th at 622; *Doe v. U.S. Air Force*, 812 F.2d at 741. Here, the government has identified no interest in the

continued retention of Armendariz's data. Indeed, the criminal case against Armendariz has been dismissed. The Fourth Amendment requires that Defendants return or destroy the copies of Armendariz's devices and the files extracted from them.

V. Defendants Are Liable Under the Colorado Constitution.

In Claim 4, Armendariz sued Summey and Ditzler for violating Article II, sections 7, 10, and 24 of the Colorado Constitution. The warrants to search and seize Armendariz's digital devices and data violated Armendariz's rights under the Colorado Constitution.

A. This Court Has Jurisdiction Over Plaintiff's Claim of Deprivation of Rights by Summey Under the Colorado Constitution.

As explained in Plaintiffs' Opposition to the United States' Motion to Substitute, ECF No. 53, Summey was acting under the direction and control of Colorado—not the FBI—when he drafted and submitted the unconstitutional warrants at issue. Substitution would be inappropriate, and Claim 4 should proceed against Summey in his individual capacity under C.R.S. § 13-21-131.

Additionally, the requirement that Armendariz exhaust administrative processes before bringing a claim should not apply here, because when this suit was filed, Armendariz did not know and had no reason to know—and still does not know—that Summey was a federal employee. *See Peden v. Winz*, No. CIV. A. 94-117, 1994 WL 180261, at *4 (E.D. La. May 4, 1994) (excusing administrative exhaustion requirement where plaintiff would not have known defendant was government employee because he did not identify himself as such); *Van Lieu v. United States*, 542 F. Supp. 862, 868 (N.D.N.Y. 1982) (echoing "the concerns of numerous judges faced with the basic unfairness of [the statute of limitations under the FTCA] when applied to genuinely ignorant plaintiffs, especially when that ignorance should have been eliminated by the responsible representation of government involvement"); *Harris v. Burris Chem., Inc.*, 490 F. Supp. 968, 971 (N.D. Ga. 1980) ("Where the driver of a motor vehicle is sued individually in state court because

the plaintiff did not know and had no reason to know that the defendant was (1) a federal employee (2) on federal business at the time of the accident and the United States subsequently removes the action to federal court under Section 2679, no exhaustion of administrative remedies is required.").

Defendants' contention that Claim 4 must be dismissed because a "private person" would not be liable for conduct analogous to Summey's is similarly unavailing. The FTCA's private analogue requirement "requires a court to look to the state-law liability of private entities, not to that of public entities, when assessing the Government's liability under the FTCA 'in the performance of activities which private persons do not perform.'" *United States v. Olson*, 546 U.S. 43, 46 (2005) (quoting *Indian Towing Co. v. United States*, 350 U.S. 61, 64 (1955)). The requirement "do[es] not restrict a court's inquiry to the same circumstances, but require[s] it to look further afield." *Id.* Thus, a claim under the FTCA for taking and searching Armendariz's devices would be analyzed under Colorado laws applicable to private persons—not to public officers. *See Stroh v. United States*, No. 11-CV-00344-LTB-BNB, 2012 WL 4069354, at *7 (D. Colo. Sept. 17, 2012) ("for the purpose of assessing FTCA applicability, I am not to review the Colorado negligence standards applicable to law enforcement officers during vehicle pursuits, but rather the liability of private persons under the circumstances.").

While Defendants are correct that C.R.S. § 13-21-131 applies to peace officers—not private persons—other statutes proscribe taking digital devices from other people's homes without permission or reason to do so, and extracting data from those devices. *See* C.R.S. § 18-4-401 ("A person commits theft when he or she knowingly obtains, retains, or exercises control over anything of value of another without authorization"); C.R.S. § 18-5.5-102 ("A person commits cybercrime if the person knowingly . . . [a]ccesses a computer, computer network, or computer system or any

part thereof without authorization [or] exceeds authorized access"). Thus, a private person could be held liable under state tort law for actions analogous to those that form the basis of Claim 4.

B. Defendants Violated the Colorado Constitution and Are Not Entitled to Qualified Immunity on Claim 4.

Armendariz brought her state constitutional claims under Colorado's Enhance Law Enforcement Integrity Act, which allows Coloradans to bring a civil cause of action for damages to vindicate violations of the state's Bill of Rights. C.R.S. § 13-21-131. Without any analysis, Ditzler argues: "For the same reasons that Armendariz fails to state federal constitutional violation claims against Officer Ditzler, she fails to allege the violation of her rights under the Colorado Constitution." (Ditzler MTD at 9.) But the Colorado Constitution "is a source of protection for individual rights that is independent of and supplemental to the protections provided by the United States Constitution." *People v. Young*, 814 P.2d 834, 843 (Colo. 1991); *see also Rocky Mt. Gun Owners v. Polis*, 2020 CO 66, ¶ 35, 467 P.3d 314, 324 (Colo. 2020) ("There is no reason to think, as an interpretive matter, that constitutional guarantees of independent sovereigns, even guarantees with the same or similar words, must be construed in the same way" (quoting Jeffrey S. Sutton, *51 Imperfect Solutions: States and the Making of American Constitutional Law* 181 (2018))).

Moreover, "qualified immunity is not a defense to liability" when officers are sued under Colorado's Enhance Law Enforcement Integrity Act. *Id.* § 131(2)(b). Even if the federal standard applied to the state law claims (which it does not), Armendariz has plausibly alleged violations of her state constitutional rights. And under state law, where officers are not entitled to qualified immunity, and Defendants have made no attempt to identify the proper standard, it is even clearer that Claim 4 cannot be dismissed.

CONCLUSION

For the foregoing reasons, Defendants' motions to dismiss should be denied.

Dated: December 18, 2023

s/ Theresa W. Benz
Jacqueline V. Roeder
Theresa Wardon Benz
Kylie L. Ngu
Davis Graham & Stubbs LLP
1550 17th Street, Suite 500
Denver, CO 80202
303-892-9400
jackie.roeder@dgslaw.com
theresa.benz@dgslaw.com
kylie.ngu@dgslaw.com

In cooperation with the ACLU Foundation of Colorado

Timothy R. Macdonald
Sara R. Neel
Anna I. Kurtz
Mark Silverstein
Laura Moraff
American Civil Liberties Union Foundation of Colorado
303 E. 17th Ave., Suite 350, Denver, CO 80203
720-402-3151
tmacdonald@aclu-co.org
sneel@aclu-co.org
akurtz@aclu-co.org
msilverstein@aclu-co.org
lmoraff@aclu-co.org

Attorneys For Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on December 18th, 2023, a copy of the foregoing was filed electronically with the Court. In accordance with Fed. R. Civ. P. 5, notice of this filing will be sent to the following parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

Anne Hall Turner
OFFICE OF THE CITY ATTORNEY OF THE CITY OF COLORADO SPRINGS
30 S. Nevada Avenue, Suite 501
Colorado Springs, CO 80903
anne.turner@coloradosprings.gov

Counsel for Defendants City of Colorado Springs, B.K. Steckler, Jason S. Otero and Roy S. Ditzler

Thomas Alan Isler
UNITED STATES ATTORNEY'S OFFICE
1801 California Street, Suite 1600
Denver, CO 80202
thomas.isler@usdoj.gov

Counsel for Defendants Daniel Summey and Federal Bureau of Investigation

s/ Beatriz Esparza
Beatriz Esparza