FILED
United States Court of Appeals
Tenth Circuit

March 12, 2026

Christopher M. Wolpert
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

FOR THE TENTH CIRCUIT

JACQUELINE ARMENDARIZ; CHINOOK CENTER,

Plaintiffs - Appellants,

v.

CITY OF COLORADO SPRINGS; DANIEL SUMMEY, in his individual capacity; UNITED STATES OF AMERICA; B.K. STECKLER, in his individual capacity; JASON S. OTERO, in his individual capacity; ROY A. DITZLER, in his individual capacity; FEDERAL BUREAU OF INVESTIGATION,

Defendants - Appellees.

CENTER FOR DEMOCRACY & TECHNOLOGY; ELECTRONIC FRONTIER FOUNDATION; ELECTRONIC PRIVACY INFORMATION CENTER; KNIGHT FIRST AMENDMENT INSTITUTE,

Amici Curiae.

No. 24-1201

Appeal from the United States District Court
for the District of Colorado
(D.C. No. 1:23-CV-01951-SKC-MDB)

Theresa Wardon Benz of Davis Graham & Stubbs LLP, Denver, Colorado (Jacqueline V. Roeder and Kylie L. Ngu, of Davis Graham & Stubbs LLP, Denver, Colorado, Timothy R. Macdonald, Sara R. Neel, Anna I. Kurtz, Mark Silverstein, and Laura Moraff, of American Civil Liberties Union Foundation of Colorado, Denver, Colorado, with her on the briefs), for Plaintiffs-Appellants.

Marissa R. Miller, Assistant United States Attorney (Matthew T. Kirsch, Acting United States Attorney, with her on the brief), Denver, Colorado, for Defendants-Appellees.

Anne H. Turner, Assistant City Attorney, Colorado Springs, Colorado, for Defendants-Appellees.

Samir Jain of Center of Democracy & Technology, Washington, DC, and Jennifer Lynch, Saira Hussain, and Brendan Gilligan of Electronic Frontier Foundation, San Francisco, California, filed an amicus brief on behalf of Electronic Frontier Foundation, Center for Democracy & Technology, Electronic Privacy Information Center, and Knight First Amendment Institute, in support of Plaintiffs-Appellants.

Before **BACHARACH**, **PHILLIPS**, and **FEDERICO**, Circuit Judges.

PHILLIPS, Circuit Judge.

In July 2021, about fifty people participated in a housing-rights march in Colorado Springs. Afterward, the Colorado Springs Police Department began to investigate the conduct of some protesters at the march. CSPD obtained three search warrants: two targeting Jacqueline Armendariz, who dropped or pushed her bike in front of a running police officer during the march; and another targeting the Chinook Center, a nonprofit that helped organize the event.

The first warrant against Armendariz allowed officers to search for and seize her electronic devices. The second warrant went a step further, allowing

officers to search for and seize a variety of data stored on those devices. The third warrant, targeting the Chinook Center, allowed officers to obtain data from the Chinook Center's Facebook profile, including all Facebook posts, chats, and events from a seven-day period.

Armendariz and the Chinook Center sued the City and several officers—Armendariz sued Detective Daniel Summey and Sergeant Roy Ditzler, and the Chinook Center sued Detective B.K. Steckler and Sergeant Jason Otero—under 42 U.S.C. § 1983, arguing that the warrants were overbroad in violation of the Fourth Amendment's particularity requirement. Armendariz also sued the FBI for retaining electronic data, seized by CSPD, in violation of the Fourth Amendment.

The Chinook Center brought related state-law claims against the City, Detective Steckler, and Sergeant Otero. Likewise, Armendariz brought state-law claims against Detective Summey and Sergeant Ditzler, though the United States later substituted itself for Detective Summey. And the Chinook Center sued the City, Detective Steckler, and Sergeant Otero for violating the Stored Communications Act, 18 U.S.C. §§ 2701–13. After four motions to dismiss, the district court dismissed the entire complaint for failure to state a claim. Armendariz and the Chinook Center timely appealed.

Exercising jurisdiction under 28 U.S.C. § 1291, we reverse the grant of qualified immunity to the officers involved with the three search warrants. Armendariz and the Chinook Center plausibly alleged that the warrants were

overbroad in violation of their clearly established right to be free from unreasonable searches and seizures. We also reverse the dismissal of Armendariz's and the Chinook Center's Fourth Amendment claims against the City.

As for Armendariz's Fourth Amendment claim against the FBI, she waived any challenge to the district court's ruling by failing to address it properly on appeal. So we affirm the district court's dismissal of that claim. For the same reason, we also affirm the dismissal of Armendariz's state-law claim against the United States. Finally, we reverse the dismissal of Armendariz's state-law claim against Sergeant Ditzler; the Chinook Center's state-law claims against the City, Detective Steckler, and Sergeant Otero; and the Chinook Center's Stored Communications Act claim.

BACKGROUND

I. Factual Background

When reviewing a decision on a motion to dismiss, we accept the complaint's well-pleaded allegations as true and consider them "in the light most favorable to the nonmoving party." *Johnson v. Smith*, 104 F.4th 153, 167 (10th Cir. 2024) (citation omitted). We may also consider "documents referred to in the complaint if the documents are central to the plaintiff's claim and the parties do not dispute the documents' authenticity." *Gee v. Pacheco*, 627 F.3d 1178, 1186 (10th Cir. 2010) (citation omitted). With that in mind, we recount

the facts as alleged in the first amended complaint and contained in the search-warrant documents attached to the motions to dismiss.

A. Tensions Between CSPD and Local Activists

The CSPD has a fraught relationship with activists in Colorado Springs. Tensions rose in the summer of 2020, when racial-justice protests erupted throughout the country in response to the police killing of George Floyd. This cause felt close to home; just one year earlier, a CSPD officer shot and killed De'Von Bailey, a nineteen-year-old Black man. In response, Jon Christiansen, Shaun Walls, and other activists founded the Chinook Center, a community hub for activists and organizations to connect and collaborate on social-justice projects.

In August 2020—on the anniversary of Bailey's death—local activists organized a protest at the home of the CSPD officer who shot Bailey. Over 100 people showed up, and some of them carried weapons. Plaintiffs allege that this protest outraged CSPD officers, sparking a "campaign" to surveil and retaliate against activists and social-justice organizations in Colorado Springs.

In fact, the day after the protest at the CSPD officer's home, an undercover CSPD officer contacted the Chinook Center's leaders. Using a fake name, the officer posed as an activist wanting to support the Chinook Center's work. From there, the officer regularly communicated with the Chinook Center's leaders and volunteered with related nonprofits. The officer gained access to various organizations' membership records, email accounts, and cell

phones. CSPD then used this information to create reports on activists and organizations connected to the Chinook Center. Plaintiffs allege that CSPD prepared these reports as part of a program called Social Media Exploitation, through which the FBI and local police gathered information from social media to monitor and target activists.

B. The Housing March and Arrests

In 2021, the Chinook Center and other local activists sought to raise public awareness of the lack of affordable housing in Colorado Springs. They organized a housing march for July 31, 2021, to coincide with the end of the federal eviction moratorium. But Colorado Springs had planned another event for that day: a parade to celebrate its 150th anniversary. These dueling events generated friction between activists and CSPD officers.

Plaintiffs allege that CSPD heard about the housing march and decided to use it as an opportunity to arrest activists. CSPD officers expressed "general animus" toward the Chinook Center and related activists:

- A CSPD commander described Walls and the Chinook Center as "instrumental" to the protest outside the home of the officer who killed Bailey. App. vol. I at 24. He called that protest a "riot," even though the Chinook Center and its leaders were never charged with any crimes connected to the protest. *Id.*
- An officer observing the march asked "why the fuck" the media cared about it. *Id.* at 25. Another officer responded that CSPD "fucked up somebody from the media," so "they care." *Id.*
- Concerned about the march disrupting the parade, an officer quipped that CSPD should "get on that bullhorn" and tell parade attendees to "stone 'em all to death" if they wanted "these motherfuckers to quit

interrupting" the parade. *Id.* Another officer responded, "Call us when we need to collect the bodies." *Id.*

- While reviewing photos of key activists, an officer stated, "Boot to the face. It's going to happen." *Id.* at 26. The officer later remarked, "Should we EPSO SWAT the shit outta these dudes and just throw flash-bangs at everyone?" *Id.* Another officer responded that they should use Stinger grenades, a less-lethal grenade often used at protests.

Against this backdrop, activists met at a local park for the housing march as scheduled. Nearby, CSPD officers waited in their police vehicles for the march to begin. A lieutenant told the officers that—if the protesters marched in the street—the officers should "mak[e] contact and effect[] arrest." *Id.* at 26.

Protesters soon left the park and started marching. At times, some of them walked in the street. When officers asked the protesters to move out of the street, the protesters complied. Even so, a CSPD commander ordered officers to arrest those protesters for obstructing traffic.

That's when officers tackled and arrested Walls, a leader at the Chinook Center. He was at the front of the march carrying a white flag with the Chinook Center's logo. Officers also arrested Christiansen, another Chinook Center leader. About fifty other people walked in the street, but the officers focused specifically on the Chinook Center's leaders.

In the meantime, Jacqueline Armendariz was walking her bike in the bike lane near the front of the march. She wore a helmet, sunglasses, and a t-shirt reading, "Housing is a human right." *Id.* at 27. After watching the officers tackle Walls, Armendariz spotted another officer running in her direction

toward the Walls fracas. At that moment, she says, she dropped her bicycle, which landed between her and the officer.[1] The officer dodged the bicycle and continued running past her. Officers did not arrest Armendariz at the march, but CSPD later reviewed video footage and asserted that she had attempted to commit second-degree assault on a police officer, a felony under Colorado law. *See* Colo. Rev. Stat. §§ 18-2-101, 18-3-203.

C. The Search Warrants

After the housing march, CSPD sought three warrants: (1) a warrant to search for and seize items from Armendariz's apartment, including her electronic devices; (2) a warrant to search for and seize data from those devices; and (3) a warrant directed at Facebook to search for and seize certain data from the Chinook Center's Facebook page. Because these warrants lie at the heart of this appeal, we describe each warrant and attached affidavit in detail.

1. First Armendariz Warrant

CSPD tasked Detective Summey with investigating the bicycle incident. After identifying Armendariz as the individual involved, Detective Summey drafted a search warrant for Armendariz's apartment, along with a supporting affidavit. The warrant incorporated an attachment listing the items CSPD would

[1] As discussed below, the search-warrant affidavits describe the bicycle incident differently from the allegations in the complaint.

search for. Mostly, the list contained items Armendariz wore during the housing march, such as her bike helmet, t-shirt, and shoes. But the affidavit also requested permission to search for and seize certain electronic devices:

> Digital media storage devices, to include phones, computers, tablets, thumb drives, and external hard drives found to be associated with Jacqueline Armendariz.

App. vol. I at 86. The warrant stated that Detective Summey had probable cause to believe these items were in Armendariz's apartment and "[w]ould be material evidence in a subsequent criminal prosecution." *Id.* at 70.

The affidavit also described the bicycle incident, the housing march, Armendariz's background, and Detective Summey's training and experience. We summarize the affidavit's discussion of each topic.

(1) Bicycle Incident: According to Detective Summey, video footage showed Armendariz riding her bicycle at the march. As an officer ran toward Walls, Armendariz got off her bike and threw it at the officer "with the clear intent to strike him with it." *Id.* at 72. The bike "nearly struck" the officer, who "had to slow his sprint" to avoid the bike. *Id.*

The affidavit thus concluded that Armendariz likely committed attempted second-degree assault, a class-five felony under Colorado law. The affidavit also included photos of the incident from body-worn camera and drone footage.

(2) Housing March: According to the affidavit, protesters at the march "immediately and intentionally walked in the roadway and obstructed traffic." *Id.* As a result, officers arrested several protesters affiliated with the Chinook

Center. The affidavit noted that the protesters had worn red shirts stating, "Housing is a Human Right," and had carried red flags. According to the affidavit, a red flag "is a radical political symbol," "designates this march . . . as revolutionary and radical in nature," and is "a symbol of socialism and communism." *Id.* The affidavit also stated that the march "was declared unlawful." *Id.*

(3) Armendariz's Background: The affidavit later detailed information about Armendariz that Detective Summey gathered from social media. Armendariz's Facebook page contained photos of her wearing the same helmet and shoes that she wore at the housing march. The affidavit then discussed Armendariz's public Twitter page, which referenced "yt supremacy." *Id.* at 82. Detective Summey described Armendariz's use of that term as "an attempt to disparage" and "show her disdain for white people." *Id.* at 83. He cited a description of "yt" from dictionary.com, which stated that "yt" derived "from the slang term *whitey*" and was "used by black Americans to disparage white people, especially implying oppression and racial discrimination." *Id.* at 82. He noted that Armendariz had attempted to assault a white officer.

(4) Training and Experience: Finally, the affidavit explained that since 2018 Detective Summey has served as a subject-matter expert on bias-motivated crimes and has investigated "illegal protest activity," including by the Chinook Center and its members. *Id.* at 71. The affidavit stated that, from his training and experience, "people 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." *Id.* at 85. It also stated that "phones regularly track the location of their user and can show where a person is at a given date and time." *Id.* And it explained that people "regularly attach their phones to their computers, and use their computers to back up their phones," and that people "store digital data on numerous devices, to include tablets, thumb drives, and external hard drives." *Id.*

Sergeant Ditzler internally approved this search warrant and affidavit, and a state judge issued the warrant. About two weeks after the march, CSPD officers searched Armendariz's apartment. They seized the items identified in the warrant, including three cell phones, two computers, and an external hard drive.[2]

2. Second Armendariz Warrant

Two days after the apartment search, Detective Summey drafted a second warrant to search the electronic devices seized from Armendariz.[3] The warrant listed the digital data that the officers intended to search for and seize:

- Photos, 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

[2] CSPD officers also obtained an arrest warrant for Armendariz and arrested her during the search.

[3] The search warrant specified each device and serial number.

> investigation. This time period 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.
>
> - key word search of the devices for the following 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, as these terms would be relevant to the investigation regardless of the time period in which they occurred.

App. vol. I at 115.[4] Detective Summey attested that the results of the keyword search "would be material evidence in the subsequent prosecution of Armendariz for attempting to assault" the officer at the housing march. *Id.* at 114.

The second search warrant's affidavit mirrored the first's, but with some important additions. For one thing, the second affidavit noted that Detective Summey spoke with Armendariz's supervisor, who confirmed that Armendariz attended the protest in her personal capacity. Next, the affidavit discussed Walls—who Detective Summey believed had "a close relationship" with Armendariz—and Walls's alarming Facebook posts. For instance, the affidavit included Facebook posts from Walls that supported violence against police officers and their families, with statements such as: "The revolution has come,

[4] We note that Detective Summey's affidavit omitted two search terms—Crustyansen and Chrischeeansen—that were included in Attachment B of the warrant, which listed the items for search and seizure.

off the pigs, time to pick up the guns," and "Kill three of [the cops'] wives or kids anywhere in the nation and watch the shit stop. Magically." *Id.* at 110–11. The affidavit also noted that Armendariz appeared on an episode of Walls's podcast focused on the August 2020 protest outside the CSPD officer's home.

Finally, the affidavit connected Armendariz's activism to her electronic devices. It described the Chinook Center as "an anarchist or anti-government organization," and it stated that "people who commit illegal activity in furtherance of the ideology or goals of anarchist or anti-government groups" often communicate electronically before or during "group activities leading up to the illegal activity." *Id.* at 106.

Once again, Sergeant Ditzler internally approved this search warrant and affidavit, and a state judge issued the warrant. Afterward, officers took Armendariz's devices to an FBI-run forensics lab. Armendariz alleges that CSPD and the FBI still retain the data they copied from her devices.

3. Facebook Warrant

Days after the housing march, Detective Steckler applied for a warrant directed at the Chinook Center's Facebook page. The warrant authorized the search and seizure of "[a]ll subscriber information tied to" the Chinook Center's "Facebook profile," including "names, phone numbers, and addresses." *Id.* at 120. It also allowed the search and seizure of certain records from a seven-day period, including the days before and after the march: (1) "All Facebook posts" from the Chinook Center's Facebook profile, (2) "All

Facebook Messenger chats tied to" the profile, and (3) "All Facebook Events" from the profile. *Id.* at 28, 120.

Detective Steckler provided a supporting affidavit. Summarized below, this affidavit recounted the housing march and its aftermath.

(1) Housing March: During the march, about sixty protesters "illegally march[ed] northbound up" the street and "block[ed] vehicle traffic in the process." *Id.* at 118. Despite "numerous verbal warnings" from the police lieutenant that their actions were illegal, the protesters kept blocking the road. *Id.* Because Walls led the group, and "extended his middle finger toward the police line," the lieutenant ordered his arrest. *Id.* Walls "actively resist[ed] the officers[']] attempts to control him by remaining on his feet and attempting to pull away from officers." *Id.* Officers eventually arrested him.

(2) March Aftermath: After the march, CSPD received an anonymous tip about a Facebook post. The post—made under Walls's name and dated the night of the housing march—read:

> Now it's fun . . . it was work before[.] I could whoop all them pigs and they felt it too. I laid down so we could keep fighting with purpose. You can watch or help idgaf. I'm going to #Fuck12.

Id. at 118–19.

A few days later, CSPD found two other Facebook profiles with information about the march. One of those profiles was for the Chinook Center. Detective Steckler attested that, in his experience, "people involved in illegal demonstrations use social media to organize planned events." *Id.* at 119. So he

believed that information from the Facebook profile would "be material evidence in this case." *Id.*

Sergeant Otero reviewed and internally approved Detective Steckler's warrant application. The affidavit stated that CSPD requested the warrant under a provision of the Stored Communications Act, 18 U.S.C. § 2703(c). A state judge signed the warrant, which CSPD then served on Facebook. Facebook complied without any notice to the Chinook Center.

D. CSPD's Policies and Practices

Finally, Plaintiffs allege that the City targeted Armendariz and the Chinook Center as part of a custom, policy, and practice. According to Plaintiffs, CSPD uses minor offenses committed at protests to expansively search individuals' digital devices and social-media accounts. These warrants allegedly target information protected under the First Amendment, rather than evidence of suspected criminal activity. Plaintiffs allege that CSPD's affidavits include conclusory statements about how protesters "send and receive photos, messages, and other information through electronic communications." And Plaintiffs complain that the officers rely solely on their "experience" and "training" for these broad assertions. They cite various search warrants directed at other activists and organizations that allegedly amount to fishing expeditions unrelated to any criminal activity.

II. Procedural Background

Soon after the housing march, Armendariz was charged for the bike incident and later pleaded guilty to obstructing a peace officer. She received a deferred judgment and served six months of unsupervised probation.

In August 2023, Armendariz and the Chinook Center sued the City, the CSPD officers responsible for their respective search warrants, and the FBI. The first amended complaint raises six claims for relief, which we categorize by type:

Claim	Plaintiff	Defendants
(I) Fourth Amendment Claims		
First Claim: Unlawful Search and Seizure, in violation of the First and Fourth Amendments, 42 U.S.C. § 1983	Armendariz	Summey, Ditzler, and the City
Second Claim: Unlawful Search and Seizure, in violation of the First and Fourth Amendments, 42 U.S.C. § 1983	The Chinook Center	Steckler, Otero, and the City
Sixth Claim: Injunctive Relief under the First and Fourth Amendments, 5 U.S.C. § 702	Armendariz	FBI
(II) Statutory and State-Law Claims		
Third Claim: Unlawful Search, in violation of the Stored Communications Act, 18 U.S.C. § 2703(a)–(b), (d)	The Chinook Center	Steckler, Otero, and the City
Fourth Claim: Deprivation of Rights, in violation of the Colorado constitution, Colo. Const. art. II, §§ 7, 10, 24; Colo. Rev. Stat. § 13-21-131	Armendariz	United States[5] and Ditzler
Fifth Claim: Deprivation of Rights, in violation of the Colorado constitution, Colo. Const. art. II, §§ 7, 10, 24; Colo. Rev. Stat. § 13-21-131	The Chinook Center	Steckler and Otero

[5] The United States moved under 28 U.S.C. § 2679(d)(1) to substitute itself for Detective Summey on the fourth claim. The magistrate judge granted the request.

Defendants filed four motions to dismiss under Federal Rule of Civil Procedure 12(b)(6).[6] Combined, these motions attacked every claim in the complaint.

The district court granted the motions, dismissed the complaint, and entered judgment. *Armendariz v. City of Colo. Springs*, No. 23-CV-01951, 2024 WL 2139316, at *1 (D. Colo. Apr. 10, 2024). Starting with the constitutional claims, the district court ruled that Plaintiffs failed to allege a plausible Fourth Amendment violation and that—even assuming a violation occurred—they never identified any clearly established law.[7] *Id.* at *4–12. So the district court held that the officers were entitled to qualified immunity for the search warrants and dismissed the Fourth Amendment claims against them. *Id.* By extension, the district court dismissed those claims against the City too. *Id.* at *13.

---

[6] The case involves four motions to dismiss: (1) Summey, the FBI, and the United States moved to dismiss the first, fourth, and sixth claims; (2) Ditzler moved to dismiss the first and fourth claims and to join the first motion; (3) Steckler and Otero moved to dismiss the second, third, and fifth claims; and (4) the City moved to dismiss the first, second, and third claims. The district court later requested and considered supplemental briefing on the officers' qualified immunity.

[7] For the first two claims, the district court also concluded that Plaintiffs failed to allege a plausible First Amendment violation. *Armendariz*, 2024 WL 2139316, at *12–13. On appeal, Plaintiffs clarify that they do not assert any freestanding First Amendment claims. Oral Arg. at 0:17:35–0:17:45. Rather, Plaintiffs invoke the First Amendment to reinforce their Fourth Amendment claims, arguing that "scrupulous exactitude" applies to search warrants implicating the First Amendment. Op. Br. at 29 (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)).

The district court then reviewed Armendariz's claim for injunctive relief against the FBI. *Id.* at *14–16. For this claim, Armendariz asserted that the FBI's retention of her digital data amounted to a Fourth Amendment violation and requested that the FBI return or destroy her data. *Id.* at *14. The district court disagreed, concluding that Armendariz failed to allege a plausible Fourth Amendment violation. *Id.* at *15. Instead, the district court determined that Armendariz should have moved for the FBI to return her property under Federal Rule of Criminal Procedure 41(g). *Id.*

The district court also dismissed the remaining claims. For the Chinook Center's Stored Communications Act claim, the court held that the Act's requirements were no more demanding than the Fourth Amendment's and thus failed for the same reasons. *Id.* at *14. The court also dismissed Armendariz's state-law claim against the United States because she failed to plead that she had exhausted the administrative process under the Federal Tort Claims Act. *Id.* at *16–17. Finally, after dismissing all the federal claims, the court found no compelling reason to exercise jurisdiction over the other state-law claims. *Id.* at *17.

Plaintiffs timely appealed.

STANDARD OF REVIEW

We review de novo a district court's decision to grant a motion to dismiss for failure to state a claim. *Stark v. Reliance Standard Life Ins.*, 142 F.4th 1252, 1256 (10th Cir. 2025). We accept all well-pleaded allegations as true and

view them in the light most favorable to Plaintiffs. *Truman v. Orem City*, 1 F.4th 1227, 1235 (10th Cir. 2021).

DISCUSSION

Plaintiffs' Fourth Amendment claims take center stage. So we start with the unlawful-search-and-seizure claims before turning to Armendariz's injunctive-relief claim and Plaintiffs' state-law and statutory claims.

I. Fourth Amendment Unlawful-Search-and-Seizure Claims (First and Second Claims)

To start, Plaintiffs appeal the district court's dismissal of their Fourth Amendment claims against the City and the officers involved in the search warrants. For each of the three warrants, the court determined that arguable probable cause supported the search and that the warrant described the search with sufficient particularity. *Armendariz*, 2024 WL 2139316, at *6–11. As a result, the court held that Plaintiffs failed to allege a plausible Fourth Amendment violation or a violation of clearly established law. *Id.* at *9–11. Thus, the district court concluded that (1) qualified immunity shielded the officers from liability, and (2) the lack of any constitutional violation defeated the municipal-liability claims against the City. *Id.* at *9–13.

On appeal, Plaintiffs argue that the district court erred in both its qualified-immunity and municipal-liability rulings. We first review whether qualified immunity protects the officers from liability for the Fourth

Amendment claims, then assess whether Plaintiffs adequately alleged these claims against the City.

A. Qualified Immunity

Qualified immunity shields officers from liability for violating a constitutional right that wasn't clearly established when the violation occurred. *Allstate Sweeping, LLC v. Black*, 706 F.3d 1261, 1266 (10th Cir. 2013). "Although qualified immunity defenses are typically resolved at the summary judgment stage, district courts may grant motions to dismiss on the basis of qualified immunity." *Thomas v. Kaven*, 765 F.3d 1183, 1194 (10th Cir. 2014). That said, defendants asserting qualified immunity through motions to dismiss face "a more challenging standard of review than would apply on summary judgment." *Id.* (citation omitted).

To survive a qualified-immunity defense at this stage in the litigation, "the plaintiff must [have] allege[d] facts sufficient to show (assuming they are true) that" (1) the "defendant plausibly violated their constitutional rights," and (2) "those rights were clearly established at the time." *Brown v. City of Tulsa*, 124 F.4th 1251, 1265 (10th Cir. 2025) (citation modified). "The plaintiff must satisfy both prongs to overcome a qualified immunity defense . . . ." *Est. of Taylor v. Salt Lake City*, 16 F.4th 744, 757–58 (10th Cir. 2021) (citation omitted).

(1) Constitutional Violation: Plaintiffs argue that the complaint plausibly alleged that the officers who crafted the three search warrants and

supporting affidavits violated the Fourth Amendment. In essence, Plaintiffs argue that the search warrants lacked the particularity necessary to pass muster under the Fourth Amendment.

The Fourth Amendment protects "against unreasonable searches and seizures." U.S. Const. amend. IV. A search or seizure is reasonable only if the warrant "particularly describ[es] the place to be searched, and the persons or things to be seized." *Id.* This particularity requirement prevents "a general exploratory rummaging of a person's belongings," *Mink v. Knox*, 613 F.3d 995, 1010 (10th Cir. 2010), and "ensures that a search is confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause," *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985).

"A warrant is overly broad if it does not contain sufficiently particularized language that creates a nexus between the suspected crime and the items to be seized." *Mink*, 613 F.3d at 1010. Without a proper nexus, a warrant violates the Fourth Amendment by "authoriz[ing] the seizure of items as to which there is no probable cause." *United States v. Cotto*, 995 F.3d 786, 798 (10th Cir. 2021) (citation omitted). Whether a sufficient nexus exists "necessarily depends upon the facts of each case." *United States v. Biglow*, 562 F.3d 1272, 1279 (10th Cir. 2009).

(2) Clearly Established: Even if Plaintiffs alleged a plausible Fourth Amendment violation, they still must demonstrate that "those rights were

clearly established at the time." *Brown*, 124 F.4th at 1265 (citation omitted). In the search-warrant context, we ask "whether there was arguable probable cause for the challenged conduct." *Stonecipher v. Valles*, 759 F.3d 1134, 1141 (10th Cir. 2014) (citation modified). An officer has arguable probable cause for a search warrant if his "conclusions rest on an objectively reasonable, even if mistaken, belief that probable cause exists." *Id.* And importantly, "a neutral magistrate judge's issuance of a warrant is the clearest indication that the officers acted in an objectively reasonable manner or in objective good faith." *Id.* (citation modified). The issued warrant generally confers a "shield of immunity" to the officers because "in the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination." *Messerschmidt v. Millender*, 565 U.S. 535, 547 (2012) (citation modified).

All that said, even when a neutral magistrate issues a warrant, an officer may still violate clearly established law in four narrow circumstances: (1) "the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth," (2) "the issuing magistrate wholly abandoned his judicial role," (3) the warrant was "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," or (4) the warrant was "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers [could not] reasonably presume it to be valid." *United*

States v. Leon, 468 U.S. 897, 923 (1984) (citation modified); *see Messerschmidt*, 565 U.S. at 547. In any of these circumstances, an officer violates clearly established law by relying on the warrant. *See Messerschmidt*, 565 U.S. at 547; *Stonecipher*, 759 F.3d at 1141–42.

With this legal framework in mind, we address whether qualified immunity protects the officers from liability for each search warrant.

1. First Armendariz Search Warrant

Armendariz argues that the complaint alleged plausible Fourth Amendment claims against Detective Summey and Sergeant Otero in relation to the first search warrant. This warrant allowed CSPD to search Armendariz's home and seize "[d]igital media storage devices, to include phones, computers, tablets, thumb drives, and external hard drives found to be associated with Jacqueline Armendariz." App. vol. I at 86.

The district court found no Fourth Amendment violation, reasoning that the warrant established probable cause for the search and seizure. *Armendariz*, 2024 WL 2139316, at *6. The court cited the affidavit's description of the alleged attempted assault, Armendariz's active use of social media, a selfie of Armendariz wearing the same bike gear that she wore during the housing march, and her association with Walls. *Id.* Yet Armendariz asserts that the warrant was overbroad because it did not explain why any of her digital devices would contain evidence of the bicycle incident.

This warrant allowed CSPD to search Armendariz's home, a location at the "very core" of the Fourth Amendment's protections. *Kyllo v. United States*, 533 U.S. 27, 31 (2001) (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)). Indeed, "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed." *United States v. Mora*, 989 F.3d 794, 800 (10th Cir. 2021) (citations omitted).

To determine whether officers had probable cause, we ask whether "a nexus . . . exist[ed] between suspected criminal activity and the place to be searched." *Id*. We consider factors such as "(1) the type of crime at issue, (2) the extent of a suspect's opportunity for concealment, (3) the nature of the evidence sought, and (4) all reasonable inferences as to where a criminal would likely keep such evidence." *Id.* at 801. To search a house for electronic devices, the warrant should contain facts supporting a reasonable belief (1) that the individual possesses the devices, (2) that the devices are in the individual's residence, and (3) that the devices contain evidence of the suspected offense. *United States v. Griffith*, 867 F.3d 1265, 1273 (D.C. Cir. 2017).

Reviewing the first search warrant and affidavit, we conclude that the officers lacked even arguable probable cause to search for and seize Armendariz's electronic devices because there was no nexus established between the bulk of the devices and the crime being investigated. In the affidavit, Detective Summey attested to his belief that Armendariz committed

second-degree attempted assault, a class-five felony under Colorado law.[8] App. vol. I at 85. Criminal attempt requires that a "person . . . act[] with the kind of culpability otherwise required for commission of [the] offense." Colo. Rev. Stat. § 18-2-101(1). And to prove second-degree assault, the government must show that the defendant acted intentionally, knowingly, or recklessly, depending on the nature of the assault. *Id.* § 18-3-203.

The affidavit explained that during the housing march, Armendariz "got off [her] bicycle and threw it at [the officer] with the clear intent to strike him with it." App. vol. I at 72. The affidavit then sought to connect the alleged crime to Armendariz's digital presence. Specifically, the affidavit included information about her online activity from open-source social media:

- Information showing that Armendariz was "associated" with Walls on Facebook;
- A selfie dated July 3, 2021, posted on Armendariz's Facebook profile, of Armendariz wearing a blue bike helmet;

---

[8] The dissent concludes "[t]he probe focused on Ms. Armendariz's possible hostility to law enforcement rather than what she had done." Dissent at 8. We acknowledge that to prove this offense, the state would have to gather evidence of Armendariz's mens rea at the time she dropped the bicycle, which is no different than all other crimes under investigation in Colorado. *Gorman v. People*, 19 P.3d 662, 665 (Colo. 2000), *as modified* (July 24, 2000), *as corrected* (May 11, 2001) ("Generally, in order to subject a person to criminal liability, there must be concurrence of the actus reus, an unlawful act, and the mens rea, a culpable mental state." (citing *People v. Torres*, 848 P.2d 911, 914 (Colo. 1993))). However, the dissent's framing of the issue and its reasoning supports Armendariz's argument that the search warrants were overbroad because they used the criminal investigation as a pretext to inquire into her "hostility to law enforcement" rather than gather evidence of an attempted assault.

- A photo dated July 19, 2021, posted on Armendariz's Facebook profile by an affiliate of the Chinook Center, of Armendariz wearing her blue bike helmet with gray Nike shoes;
- A second photo of Armendariz posted by the same nonprofit showing her in the same shoes and helmet with a bicycle;
- A podcast episode, dated July 28, 2021, during which Armendariz discussed the importance of affordable housing; and
- Active Facebook, Twitter, and LinkedIn profiles that suggested Armendariz was "very active politically."

Id. at 78–84.

This information in the affidavit supports a reasonable belief that Armendariz had an online presence on social media, a reasonable inference that she possessed and used *some* electronic devices to take photos and participate in social media and that she may have kept the devices in her home. The affidavit also described Detective Summey's training and experience, including his knowledge about "people who engage in illegal protest activity," their phone usage, and their storage of digital data on multiple devices. *Id.* at 85. Detective Summey's training and experience thus attempted to connect Armendariz's devices to evidence of her conduct at the march and her intent when she dropped or threw her bicycle. Finally, we note that a state judge signed and issued the warrant that the officers relied on to seize the six devices. *Id.* at 69, 85.

Under these circumstances, we cannot conclude that Detective Summey's affidavit established the required nexus between Armendariz's suspected

criminal activity at the protest and the search of her home for various electronic devices. "The Fourth Amendment allows a search for evidence when there is probable cause to believe that the evidence sought will aid in a particular apprehension or conviction." *Messerschmidt*, 565 U.S. at 551 (citation modified). But an officer could not reasonably believe that the information in Armendariz's devices, if any information existed and whatever those devices may be, would further an investigation into the spontaneous attempted assault that happened at a certain time and place away from her home.

For one, the affidavit supported that Armendariz was active on social media, but it required an inference that she possessed the electronic devices that were listed to be seized. Second, the affidavit relied solely on Detective Summey's "training and experience" about "people who engage in illegal protest activity" to establish a nexus between the electronic devices and the assault under investigation. This purported nexus is extremely flimsy and speculative. As we said in *Mora*, "[a]llowing officers to search a home based solely on an affiant's experience and pure speculation would perpetuate that evil (which the Fourth Amendment is directed against)." 989 F.3d at 800.

In *Mora*, we considered whether a search warrant established a sufficient nexus between the suspected criminal activity and the defendant's residence. *Id.* at 800. Officers arrested the defendant for alien smuggling and found a gun safe during a protective sweep of his home. *Id.* at 798. The officers then obtained a warrant to search the house for evidence of alien smuggling and

possessing a firearm as a felon. *Id.* We determined that the protective sweep violated the Fourth Amendment and thus reviewed whether the search warrant—absent information about the gun safe—provided probable cause for the search. *Id.* at 799–800. The government relied on conclusory statements in the search-warrant affidavit that "alien smugglers often use electronic communication devices, GPS devices, and electronic banking systems to conduct operations and store records." *Id.* at 801. We held that these statements failed to provide probable cause because none were "specific to Defendant's crime or circumstances." *Id.*

Like in *Mora*, the affidavit here did not contain facts connecting the criminal activity under investigation to the electronic devices. The affidavit included information about Armendariz's active online presence; her public postings about her social-justice activism; photos of her at an event posted by a nonprofit affiliated with the Chinook Center; and her Facebook connection to Walls. At most, the officers had reason to believe by inference that Armendariz had a cell phone on her possession at the protest (which is reasonable given the ubiquity of cellphones and the "selfies" she posted online), so it also may contain evidence of her presence at the housing march and possibly her mens rea during the bicycle incident.

But the warrant went well beyond seizing the phone. It allowed officers to seize a long list of electronic devices on the theory that Detective Summey "is also aware that people regularly attach their phones to their computers, and

use their computers to back up their phones, or transfer photos from their phones to save space on their phones. Your Affiant knows that people store digital data on numerous devices, to include tablets, thumb drives, and external hard drives." App. vol. I at 85. This justification is entirely speculative, relying on purported knowledge—entirely without foundation—of how "people," in general, act. Further, it relies on an antiquated view of how people use their cell phones with other electronic devices. Regardless, it is insufficient to establish the nexus between all the electronic devices and the crime under investigation, as the law demands.

Similarly in *Griffith*, officers investigated the defendant for a year-old gang-related homicide. 867 F.3d at 1268. Officers obtained a warrant to search his apartment and seize any cell phones and electronic devices found there. *Id.* at 1269–70. The D.C. Circuit concluded that the warrant was overbroad. To begin, the affidavit never explained that the defendant likely owned a cell phone. *Id.* at 1272–73. Nor did it explain whether a cell phone "would be located in the home and would contain incriminating evidence about [the] suspected offense." *Id.* at 1273. Plus, the warrant permitted the seizure of any electronic device regardless of who owned it. *Id.* at 1276. The D.C. Circuit highlighted how these electronic devices were lawful items, not contraband, and cautioned against "a blanket authorization" to seize "innocuous objects." *Id.* (citation modified).

Though the warrant here did identify Armendariz as a social media user, it contained the same infirmities as the *Griffith* affidavit and was in essence "a blanket authorization" to seize all electronic devices without any showing they may contain evidence of the crime under investigation. As the *Griffith* court noted, "there is no commonsense reason simply to presume that individuals own a computer or a tablet. Those sorts of devices do not approach cell phones in their ubiquity[.]" *Id*. at 1272.

The dissent's reasoning rests heavily upon a factual predicate that Armendariz possessed a cellphone, which it then uses as the gateway to all the other electronic devices listed in the warrant. But this conclusion assumes that the warrant is severable and that we could or should break it apart based upon the items listed in the warrant to be searched for and seized. The parties did not argue or discuss severability of the warrant, so the dissent's assumption is molded from its own clay. Moreover, as best we can tell, this court has never held the severability doctrine applies in a civil case.

In *Cassady v. Goering*, we declined to decide whether the doctrine applied in a civil case because the court concluded that the severability doctrine would not apply to that case even if it were an appeal from a criminal suppression hearing. 567 F.3d 628, 637 (10th Cir. 2009). The court then proceeded through a lengthy analysis of the severability doctrine as if considering a criminal case. Here, the parties did not argue the severability

doctrine, which the dissent raises. The dissent simply concludes that the doctrine applies and that the warrant is severable.

In the criminal context, courts apply the severability doctrine in determining the scope of the exclusionary rule. *United States v. Sells*, 463 F.3d 1148, 1155 (10th Cir. 2006). But in the civil context, the exclusionary rule is not at issue. Instead, a jury is tasked at the liability phase to make a binary determination of whether the warrant violated the Fourth Amendment at all. We decline to adopt the dissent's approach or to consider whether there are valid parts of the warrant here (for instance, the dissent mentions severing the cellphone) from the invalid parts of the warrant.

For these reasons, we conclude that the officers lacked even arguable probable cause to seize Armendariz's electronic devices that were listed in the search warrant. And so, Armendariz has alleged a clearly established Fourth Amendment violation related to the first warrant. *See Stonecipher*, 759 F.3d at 1141.

Even with that conclusion, we must consider whether the state judge's issuance of the warrant overcomes our misgivings as to its legality under the Fourth Amendment. After all, "[a] neutral magistrate judge's issuance of a warrant is the clearest indication that the officers acted in an objectively reasonable manner or in objective good faith." *Id.* (citation modified). Still, we conclude that Armendariz plausibly alleged that the officers violated clearly established law, because the facts alleged support that the warrant was "so

facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers c[ould not] reasonably presume it to be valid." *Leon*, 468 U.S. at 923. We therefore reverse the district court's ruling that qualified immunity protects Detective Summey and Sergeant Ditzler from liability for this search warrant.[9]

2. Second Armendariz Search Warrant

Armendariz also challenges the second warrant authorizing the search and seizure of data from her electronic devices. She contends that the search-warrant affidavit turned the warrant into a "wide-ranging fishing expedition for political views and associations." Op. Br. at 20. The district court concluded otherwise, holding that the officers had at least arguable probable cause for the search warrant and that the warrant met the particularity requirement. *Armendariz*, 2024 WL 2139316, at *6–8.

We review the second search warrant under each qualified-immunity prong. In doing so, we conclude that Armendariz alleged a plausible Fourth

[9] The complaint suggests that CSPD officers had ulterior motives for obtaining the warrant. But that does not impact whether the warrant provides arguable probable cause. *See Ashcroft v. al-Kidd*, 563 U.S. 731, 739 (2011). And though the complaint suggests that the officers acted in bad faith, Plaintiffs do not argue that the officers' alleged motives led to false statements in the search warrants. *See generally Franks v. Delaware*, 438 U.S. 154, 155–56 (1978) (requiring the suppression of evidence obtained through false statements in a search warrant); *Leon*, 468 U.S. at 923 (same).

Amendment violation and reverse the district court's dismissal of this part of her claim.

a. Constitutional Violation

As discussed, the Fourth Amendment requires that a warrant "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "A warrant is overly broad if it does not contain sufficiently particularized language that creates a nexus between the suspected crime and the items to be seized." *Mink*, 613 F.3d at 1010. We focus on "practical accuracy rather than technical precision" when considering whether a search warrant satisfies the particularity requirement. *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (citation omitted). And at bottom, "[t]he 'touchstone' of the Fourth Amendment is 'reasonableness.'" *Biglow*, 562 F.3d at 1279 (quoting *Samson v. California*, 547 U.S. 843, 855 n.4 (2006)).

In the context of digital searches, we have recognized that "enormous amounts of information and relevant evidence can be stored" on digital devices. *United States v. Palms*, 21 F.4th 689, 698 (10th Cir. 2021). It follows that searching these devices can provide significant access to an individual's private affairs. *Otero*, 563 F.3d at 1132. To protect against unwarranted intrusions, "the Fourth Amendment requires warrants for computer searches to affirmatively limit the search to evidence of specific crimes or specific types of material." *Palms*, 21 F.4th at 698 (citation modified). In other words, warrants to search digital devices must contain a "limiting principle" that "establish[es]

practical guidelines about what can be searched and seized, leaving nothing to the discretion of the officers executing the warrant." *Id.* (citation omitted).

For the second search warrant, Armendariz contends that two aspects of the warrant violated the Fourth Amendment's particularity requirement: the keyword search and the file search. We consider each in turn.

(1) Keyword Search: Armendariz argues that the warrant's keyword search lacked particularity because it was overbroad. The warrant allowed officers to search Armendariz's six devices for these keywords:

> 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, as these terms would be relevant to the investigation regardless of the time period in which they occurred.

App. vol. I at 115.

We agree with Armendariz that this keyword search failed to include sufficient limits under the Fourth Amendment's particularity requirement. We detect several problems with the keyword search that contribute to the warrant's overbreadth.

First, the keyword search failed to limit the search and seizure to evidence related to the crime under investigation. Consider the type of information that would fall within this search warrant's scope:

- Discussions about any "protest," without reference to which protest or what is being protested;

- Discussions about any "officer," "cop," or "pig," regardless of whether the terms refer to police brutality or an actual animal;
- Armendariz's communications with or about any of the Chinook Center's founders and with or about anyone who shares their names;
- Any reference to the word "right," regardless of whether the communication refers to a human right or simply expresses agreement; and
- Any reference to an assault, regardless of which one.

Certainly, the keyword search allowed officers to search for and seize data completely unrelated to any crime. The warrant's failure to limit the search to evidence of the attempted assault contributes to its lack of particularity. *See, e.g., Mink*, 613 F.3d at 1010–11 (holding that a search warrant was overbroad because it failed to limit the search to evidence of a specific crime); *cf. United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) (holding that a search warrant met the particularity requirement in part because it limited the search of computer records to evidence of drug trafficking); *United States v. Brooks*, 427 F.3d 1246, 1252–53 (10th Cir. 2005) (same, where the warrant "naturally" limited the search of digital devices to evidence of child pornography).

Second, the officers had enough information to narrow the search warrant's scope but chose not to do so. "Failure to employ the specificity available will invalidate a general description in a warrant." *United States v. Leary*, 846 F.2d 592, 605 (10th Cir. 1988) (citation omitted). In *Leary*, officers obtained a search warrant while investigating the defendants' illegal export

scheme. *Id.* at 594. The warrant allowed officers to search for and seize "a long list of business records typical of the documents kept by an export company" so long as the records "relate[d] to the purchase, sale and illegal exportation of materials in violation of the federal export laws." *Id.* at 600–01 (citation modified). We held that the warrant was facially overbroad in part because "information was available to the government to make the description of the items to be seized much more particular." *Id.* at 604. For instance, the government could have narrowed the search to documents related to the suspect transaction, companies suspected of illegal export activity, or countries that were part of the export route. *Id.*

Like the warrant in *Leary*, the warrant's keyword search failed to sufficiently narrow the data to be searched and seized. For example, though the crime under investigation dealt with a discrete incident occurring on July 31, 2021, the keyword search specifically disclaimed any temporal limit on the data for search and seizure. True, the warrant stated that the keywords "would be relevant to the investigation regardless of the time period in which they occurred." App. vol. I at 115. Yet the affidavit did not explain *why* all data involving these keywords—including communications made years before the housing march—would be relevant to the alleged attempted assault. What's more, the keyword search identified individuals unrelated to the alleged assault, such as Jon and Samantha Christiansen. Granted, these individuals were affiliated with the Chinook Center and the housing march. But the absence of

any other limiting principle connecting their names to the attempted assault renders these search terms overbroad. All in all, the officers did not narrow the keyword search using available information, making the warrant overbroad. *See United States v. Blakeney*, 942 F.2d 1001, 1027 (6th Cir. 1991) (concluding that a warrant was overbroad when it described the items for seizure as "jewelry" when the officers had a specific inventory of stolen items from the jewelry store).

Third, the keyword search failed to distinguish between the data officers could *search for* and the data officers could *seize*. The warrant allowed officers to seize any data responsive to the keyword search—even if the search returned data unrelated to the crime under investigation. We cannot endorse such a broad authorization. Doing so would transform minor crime investigations into opportunities to seize a wide range of information unrelated to the conduct at issue. *See Leary*, 846 F.2d at 602 (holding that warrants must "allow the executing officers to distinguish between items that may and may not be seized"); *United States v. Russian*, 848 F.3d 1239, 1245–46 (10th Cir. 2017) (holding that a warrant was overbroad for not identifying what material the officers could seize).

In *United States v. Zelaya-Veliz*, the Fourth Circuit addressed the "distinction between what may be searched and what can be seized" in the context of warrants for digital data. 94 F.4th 321, 337 (4th Cir. 2024). It endorsed a two-step approach for maintaining that distinction. *Id.* at 337–38

(citing Fed. R. Crim. P. 41(e)(2)(B) advisory committee's note to 2009 amendment). At step one—the search—officers may obtain and sift through a broader array of digital data. *Id.* at 338. Like any search, the officers will encounter information irrelevant to the crime. *Id.* At step two—the seizure—the officers may "seize only the fruits, evidence, or instrumentalities of the crimes for which they had established probable cause." *Id.*

But here, the warrant never distinguished between the search and the seizure. Instead, it allowed officers to seize all data responsive to the keyword search. Given the broad scope of the search—which encompassed any message with "right," "bike," or "housing"—the search would inevitably return data unrelated to the attempted assault. Without any principle limiting the data officers could seize, the warrant failed to protect against serious intrusions into Armendariz's privacy. This failure adds to the warrant's overbreadth.

Defendants make several arguments against finding a Fourth Amendment violation. None are persuasive. First, Defendants argue that Detective Summey's affidavit identified the crime at issue and explained how Armendariz became a suspect. So according to Defendants, incorporating the affidavit remedied any lack of specificity. We agree that a properly incorporated affidavit can cure a warrant's lack of particularity. But that's not the case here.

An affidavit can remedy a defective search warrant if "(1) the warrant and the affidavit [are] attached; and (2) the warrant . . . expressly incorporate[s] the affidavit." *United States v. Suggs*, 998 F.3d 1125, 1135 (10th

Cir. 2021). But when a warrant is overbroad, the incorporated affidavit must introduce a limiting principle. *See United States v. Sadlowski*, 948 F.3d 1200, 1205 (10th Cir. 2020) (concluding that a search warrant met the particularity requirement where it permitted a search of the residence "described in the affidavit" (citation modified)); *United States v. Kahre*, 737 F.3d 554, 566–67 (9th Cir. 2013) (same, where a search warrant for "all records" incorporated an affidavit that limited the search to "records" from "the period January 1, 1992, until December 31, 1993; and January 1, 1997 to present date").

The affidavit attached to the second warrant provided no such limiting principle. The warrant attached and expressly incorporated Attachments A and B. *See Suggs*, 998 F.3d at 1135. Attachment A was the supporting affidavit; Attachment B identified the file search and keyword search. App. vol. I at 91, 115. But despite incorporating both attachments, the warrant identified only Attachment B for the "property or thing(s) [that] will be searched for and, if found, seized." *Id.* at 87.

At no point did the warrant or Attachment B state that the affidavit limited the scope of the search or seizure. *See Sadlowski*, 948 F.3d at 1205 (warrant expressly incorporated the affidavit's description of the residence as the place to be searched); *Kahre*, 737 F.3d at 566–67 (same for the affidavit's timeframe, which limited the records to be searched). Instead, the warrant made clear that Attachment B, not the affidavit, defined the boundaries of the search and seizure.

Plus, even considering the affidavit, we fail to see how descriptions of the bicycle incident and various social-media posts amounted to a clear limiting principle on the scope of the search. Instead, the affidavit merely recounted the evidence that the officers believed formed the probable cause necessary for the search and seizure. That did not limit the scope of the keyword search, such that "nothing [was] left to the discretion of the officer executing the warrant." *Stanford v. Texas*, 379 U.S. 476, 485 (1965) (citation omitted).

Besides missing a limiting principle, parts of the affidavit directly contradicted the scope of the keyword search as stated in Attachment B. For example, the affidavit focused on the timeframe surrounding the attempted assault on July 31, 2021. But the keyword search disregarded this limit, stating that the search "terms would be relevant to the investigation regardless of the time period in which they occurred." App. vol. I at 115. To accept Defendants' argument that the affidavit limited the scope of the search and seizure would be to condone searches with murky boundaries and nebulous scopes. That result would frustrate the Fourth Amendment's proscription against warrants that allow "exploratory rummaging," *Mink*, 613 F.3d at 1010, or "authorize[] the seizure of items as to which there is no probable cause," *Cotto*, 995 F.3d at 798

(citation omitted). In sum, the affidavit fails to narrow the warrant's broad scope.[10]

Next, Defendants argue that the particularity requirement doesn't even apply to the keyword search. According to Defendants, the keyword search merely limited how officers could conduct the search. Put differently, they argue that the keyword search was only a search strategy, which need not meet the Fourth Amendment's particularity requirement.

Again, Defendants correctly state the law but misapply it to the warrant at issue. To comply with the Fourth Amendment, "a warrant must describe with particularity the items sought on a computer," but "need not include a particularized computer search strategy." *United States v. Wagner*, 951 F.3d 1232, 1247 (10th Cir. 2020) (citation modified); *see Russian*, 848 F.3d at 1245 n.1 (rejecting a "search methodology requirement" that would require law enforcement "to specify an ex ante search protocol before a warrant could issue" for digital devices). Thus, a preauthorized computer-search strategy does not affect whether a warrant meets the Fourth Amendment's particularity requirement.

---

[10] Defendants point to the affidavit's statement that the keyword search "would be material evidence in the subsequent prosecution of Armendariz for attempting to assault [the] [o]fficer." App. vol. I at 114. They claim that this language limited the scope of the search to evidence of the attempted assault. Yet the cited language did not restrict the keyword search. It merely commented on the materiality of the evidence responsive to the search. So we reject Defendants' position that this language cures the warrant's overbreadth.

Here, though, Defendants improperly equate the items for seizure with a computer-search strategy. The record belies this position. The warrant itself listed the keyword search under "property or thing(s) [that] will be searched for and, if found, seized." App. vol. I at 87; *see id.* at 115. Nowhere did the warrant state that officers should perform the keyword search and then cabin the items seized to evidence of the attempted assault.[11] Instead, the warrant authorized the seizure of *all* data responsive to the keyword search. With this in mind, we decline to characterize the keyword search as a computer-search strategy.[12]

---

[11] We considered whether we could construe the keyword search as a computer-search strategy that controlled how the officers went about the file search. But the keyword search's language directly contradicts this reading. Though the warrant limited the file search to data "for the time period of 6/5/2021 through 8/7/2021," the keyword search specified that the "terms would be relevant to the investigation regardless of the time period in which they occurred." App. vol. I at 115. So the warrant's plain language establishes that the keyword search was separate from—rather than a search methodology for—the file search.

[12] Defendants also argue that Armendariz should have challenged the reasonableness of the search instead of the warrant's particularity. They assert that, by never raising reasonableness, Armendariz forfeited her challenge to the keyword search. True enough, this argument carries weight if the keyword search was a search methodology. In that case, Armendariz should have challenged the reasonableness of the search, not the warrant's particularity. *See Palms*, 21 F.4th at 700–01 & n.12. But because we determine that the keyword search described the items to be searched and seized, not how to conduct the search, we conclude that Armendariz properly challenged the warrant's particularity.

For all these reasons, we conclude that Armendariz has plausibly alleged that the keyword search was overbroad. Though the keyword search alone violates the Fourth Amendment, we review the warrant's file search as well.

(2) File Search: Armendariz also asserts that the warrant's file search was overbroad. That part of the warrant allowed the search and seizure of certain files:

> Photos, 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. This time period 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.

App. vol. I at 115.

From the start, we note that many of the problems with the keyword search plague the file search as well. And so, like the keyword search, the file search was overbroad. We highlight several aspects of this search that contribute to its overbreadth.

First, the warrant sought location data from June 5, 2021, through August 7, 2021. But neither the warrant nor the affidavit explained why probable cause existed to search for and seize any data beyond Armendariz's location at the time of the attempted assault. *Cf. United States v. Barajas*, 710 F.3d 1102, 1109 (10th Cir. 2013) (doubting that an affidavit's description of the defendant's cell-phone use for a drug-trafficking conspiracy would provide sufficient

probable cause to search for GPS data). The Supreme Court has recognized the sensitive nature of location data: it "provides an intimate window into a person's life, revealing not only [her] particular movements, but through them [her] familial, political, professional, religious, and sexual associations." *Carpenter v. United States*, 585 U.S. 296, 311 (2018) (citation modified). Because the officers knew the date and time of the alleged assault, it is unclear why the officers had probable cause to search for and seize location data from a two-month period. *Cf. Leary*, 846 F.2d at 605.

Similarly, the file search encompassed photos, videos, messages, and emails during the specified timeframe. Again, despite the brief interaction between Armendariz and the officer she allegedly tried to assault, the warrant authorized the search and seizure of a wide range of files outside the timeframe of the interaction. The affidavit did not explain why a two-month period would be needed for this alleged attempted assault. Without additional limits on the scope of the search and seizure, we conclude that this two-month period was overbroad.

Defendants retort that the file search included certain qualifying phrases limiting the search's scope. They emphasize that the warrant referred to files "that are determined to be *relevant to this investigation*," and that the timeframe "would allow for any planning *leading up to the crime* . . . and the subsequent taking of credit for *committing a violent act against a police*

officer." App. vol. I at 115 (emphasis added). Thus, Defendants argue that these statements limited the search and seizure to evidence of the attempted assault.

We disagree. We acknowledge that the first phrase—items "that are determined to be relevant to this investigation"—limited the file search to "this investigation." But the affidavit did not sufficiently dispel the ambiguity inherent in the term "investigation." Though Defendants argue that the "investigation" related to the attempted assault, the affidavit reflected a broader investigation into the Chinook Center, individuals associated with the Chinook Center, and Armendariz's background and political views. *See id.* at 92, 102–05. Rather than limit the scope of the file search, the affidavit confirms its expansive reach.

The other mentions of the search's timeframe also did not limit the warrant's scope. The warrant's use of "the crime" and "committing a violent act against a police officer" adds to the confusion because the affidavit also referenced "illegal protest activity" and an "unlawful" march. *Id.* at 92, 105. And so, the search warrant allowed officers to seize evidence related to the housing march overall, not just the attempted assault.

Thus, under "a common sense and realistic" reading of the warrant and affidavit, the warrant allowed a search and seizure of evidence beyond that of the attempted assault. *See United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006); *Suggs*, 998 F.3d at 1133 (rejecting a warrant as overbroad that permitted the search and seizure of "any item identified as being involved in

the [crime]" (citation omitted)). We reject Defendants' invitation to treat this ambiguous language as sufficient to guard against overbreadth. Doing so would give undue discretion to the officer executing the warrant. *See Stanford*, 379 U.S. at 485.

We aren't persuaded by Defendants' other arguments, either. They argue that we should narrowly construe words or expressions in warrants that might be read expansively. But in the cases Defendants rely on, the warrants all contained other language that limited the scope of the authorized searches—unlike here.

In *Burgess*, we upheld the validity of a search warrant for "computer records" because other language in the warrant limited the search to "pay-owe sheets, address books, rolodexes," and "personal property which would tend to show conspiracy to sell drugs." 576 F.3d at 1091 (citation omitted). Likewise, in *Wagner*, we upheld a search warrant that delineated sixteen categories of items for seizure, even though some of the categories were open-ended. 951 F.3d at 1248. We reasoned that the warrant "contained sufficiently particularized language requiring a nexus with child pornography" to restrict those few categories that did not reference a specific subject matter. *Id.* (citation omitted).

Even better, the warrants' opening language in *Brooks*, *Palms*, and *United States v. Christie* expressly limited the searches and seizures to evidence of criminal activity. *Brooks*, 427 F.3d at 1252 (permitting a search of

two computers and some disks "for evidence of child pornography" (citation omitted)); *Palms*, 21 F.4th at 694, 697–98 (similar, for "evidence of human trafficking" (citation modified)); *Christie*, 717 F.3d 1156, 1165 (10th Cir. 2013) (similar, for "all records and information relating to the murder, neglect, and abuse" of a specific person between specific dates (citation modified)). By contrast, the second warrant here contained no comparable language limiting the search and seizure to evidence of the attempted assault.

We therefore hold that Armendariz alleged a plausible Fourth Amendment violation for the second search warrant. At bottom, this warrant authorized a far-reaching search and seizure of digital data for an alleged assault that occurred at a known, specific moment in time. We decline to permit "wide-ranging exploratory searches" of digital data merely because a minor crime with an intent requirement occurred at a protest.[13] *Palms*, 21 F.4th at 698 (citation omitted).

b. Clearly Established

Though Armendariz has alleged a plausible Fourth Amendment violation, Detective Summey and Sergeant Ditzler argue that qualified immunity still protects them from liability because they did not violate a clearly established

[13] For this warrant, Armendariz also argues that the First Amendment requires "scrupulous exactitude" when analyzing her Fourth Amendment claims, because the search targeted her political speech. Because we conclude that Armendariz pleaded a plausible Fourth Amendment violation, we need not consider the First Amendment's implications in this appeal.

right. The district court agreed. *Armendariz*, 2024 WL 2139316, at *9–10. On appeal, Armendariz contends that the district court was mistaken.[14]

We rely on four cases to conclude that the officers violated clearly established law: *Mink*, *Leary*, *Voss*, and *Cassady*. To begin, in *Mink* we held that "it was . . . clearly established that warrants must . . . meet the particularity requirement of the Fourth Amendment in order to be constitutionally valid." 613 F.3d at 1011. Indeed, "[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 v. Ramirez*, 540 U.S. 551, 563 (2004). *Mink* thus leaves little doubt that the Fourth Amendment's particularity requirement is clearly established law. *See* 613 F.3d at 1011.

Next, *Leary*, *Voss*, and *Cassady* underscore that no officer could have "reasonably presume[d]" the warrant here "[was] valid." *Leon*, 468 U.S. at 923. All three cases held that warrants without sufficient limiting principles lack particularity. *See Leary*, 846 F.2d at 602, 605–06; *Voss*, 774 F.2d at 404–05;

[14] The dissent concludes that Armendariz waived her appellate argument about a clearly established violation because she did not "address the clarity of a violation involving the provisions in the first warrant to allow the seizure of the digital devices." Dissent at 7. In other words, as we understand the dissent, Armendariz needed to argue how the law was clearly established for each device mentioned in the warrant to avoid appellate waiver. This again depends on the warrants being severable, a point unraised by the defendants and thus subject to waiver. We disagree with the dissent's finding waiver by the plaintiff based on an invalid legal premise waived by the defendants.

Cassady, 567 F.3d at 636. And as explained, that's the case here. The second search warrant failed to "establish practical guidelines about what can be searched and seized, leaving nothing to the discretion of the officers executing the warrant." *Palms*, 21 F.4th at 698. Instead, it allowed officers to search and seize an array of data unconnected to the attempted assault. Our caselaw therefore supports that Armendariz has alleged a plausible violation of her clearly established rights.

Defendants argue that our decisions in *Brooks*, *Palms*, and *Christie* should sway us otherwise. But as we already explained, all three cases are distinguishable for the same reason: those warrants limited the searches and seizures to evidence of the crime at hand. *See Brooks*, 427 F.3d at 1252; *Palms*, 21 F.4th at 697–98; *Christie*, 717 F.3d at 1165. Again, the warrant here contained no such limit.

As in *Cassady*, "[i]n light of our conclusion that the warrant was impermissibly overbroad, the clearly established prong is easily satisfied." 567 F.3d at 643–44. We conclude that Armendariz plausibly alleged that Detective Summey and Sergeant Ditzler violated her clearly established right to be free from unreasonable searches and seizures.

3. Facebook Search Warrant

We turn now to the Facebook warrant directed at the Chinook Center, which allowed officers to search and seize certain categories of Facebook data. The district court held that the Chinook Center failed to allege any plausible

Fourth Amendment violation for this warrant. *Armendariz*, 2024 WL 2139316, at *11–12. Alternatively, the district court concluded that any Fourth Amendment violation did not violate clearly established law. *Id.* at *11. On appeal, the Chinook Center contends that the district court erred on this issue and asks us to reverse the dismissal of its Fourth Amendment claim.[15] We first review the alleged constitutional violation and then turn to whether that violation was clearly established.

a. Constitutional Violation

The Chinook Center argues that this warrant was overbroad because the warrant failed to establish a nexus between the Chinook Center's Facebook account and any crime.[16] As discussed, the search warrant targeted certain information from the Chinook Center's Facebook account:

> All subscriber information tied to Facebook profile: https:www.facebook.com/chinookcenter to include names, phone numbers, and addresses.

---

[15] Defendants do not challenge the Chinook Center's Fourth Amendment standing. And because Fourth Amendment "standing" is not jurisdictional, we need not address the issue. *United States v. White*, 584 F.3d 935, 952 n.7 (10th Cir. 2009).

[16] The Chinook Center also argues that the warrant did not identify a crime under investigation or establish that illegality pervaded the housing march. We disagree. First, the affidavit specified the crimes under investigation: "Obstructing Passage or Assembly, and Resisting, Interference with a Public Official." App. vol. I at 118. Second, the affidavit provided a factual basis for the allegedly pervasive illegality at the march by asserting that the "60 protesters illegally march[ed]," ignored "numerous verbal warnings" to move out of the street, and "block[ed] vehicle traffic." *Id.*

> All Facebook posts for profile:
> https:www.facebook.com/chinookcenter from 07/27/21 to 08/02/21.
>
> All Facebook Messenger chats tied to Facebook profile:
> https:www.facebook.com/chinookcenter from 07/27/21 to 08/02/21.
>
> All Facebook Events for profile:
> https:www.facebook.com/chinookcenter from 07/27/21 to 08/02/21.

App. vol. I at 120. The district court concluded that this warrant was "sufficiently particular" because it limited the search to evidence from a seven-day period and "involv[ed] specific arrests for specific infractions all occurring on July 31, 2021." *Armendariz*, 2024 WL 2139316, at *11.

We disagree and conclude that this warrant, too, violates the Fourth Amendment for overbreadth. As discussed, warrants to search computers and other digital devices present significant Fourth Amendment dangers. In effect, digital devices "store and intermingle a huge array of one's personal papers in a single place." *Otero*, 563 F.3d at 1132. To prevent unwarranted intrusions into these devices, we have instructed that "warrants for computer searches must *affirmatively limit* the search to evidence of specific federal crimes or specific types of material." *Id.* (citation omitted).

Some courts have expressed heightened concern when warrants involve Facebook. *See, e.g., United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017); *United States v. Shipp*, 392 F. Supp. 3d 300, 308 (E.D.N.Y. 2019). And rightly so. Facebook warrants risk significant Fourth Amendment intrusions.

First, "Facebook provides a single window through which almost every detail of a person's life is visible." *Shipp*, 392 F. Supp. 3d at 308. Users "voluntarily entrust information" to Facebook on "just about every aspect of their lives," and Facebook "proactively collects and aggregates information about its users." *Id.* Put differently, Facebook may have more data about its users than those users voluntarily store for themselves.

Second, unlike hard drives or other digital devices, Facebook carefully categorizes and sorts the user's data. *Id.* at 309. That eliminates certain compelling reasons for a broad data search. *Id.* "The means of hiding evidence on a hard drive—obscure folders, misnamed files, encrypted data—are not currently possible in the context of a Facebook account." *Blake*, 868 F.3d at 974. Also, a digital-device warrant often entails a time-consuming search of digital data with special forensic equipment. *Id.* A Facebook search, on the other hand, requires only that the government request the desired data from Facebook. *Id.*

Because of these differences in storing, categorizing, and searching data, broad requests to search and seize Facebook data merit particular scrutiny. With these principles in mind, we turn to the warrant at issue here.

To start, the warrant permitted the search and seizure of all subscriber information tied to the Chinook Center's Facebook profile, including names, phone numbers, and addresses. App. vol. I at 120. Yet even the Stored Communications Act contemplates disclosure of this information. *See* 18

U.S.C. § 2703(c). We see no Fourth Amendment issue with the request for subscriber information on these facts, nor does the Chinook Center argue otherwise.

Next, the warrant requested the search and seizure of all Facebook posts, Facebook Messenger chats, and Facebook Events from July 27, 2021, to August 2, 2021 (the days just before and after the march). App. vol. I at 120. As the district court recognized, including a timeframe significantly narrows the scope of the search and seizure. *See Armendariz*, 2024 WL 2139316, at *11; *Blake*, 868 F.3d at 974 ("[T]he warrants should have requested data only from the period of time during which [the defendant] was suspected of taking part in the [crime].").

At the same time, the warrant allowed CSPD to search for and seize *all* Facebook posts, Facebook Messenger chats, and Facebook Events, regardless of their relation to the crimes at issue. Despite the difficulty of sorting and searching through data, various cases show that officers can particularize their requests for information from Facebook. For example, the officers could have narrowed the search by limiting "the request to messages sent to or from persons suspected" of committing the crimes, *Blake*, 868 F.3d at 974, or to "evidence, fruits, and instrumentalities of the specified offenses," *United States v. Ulbricht*, 858 F.3d 71, 104 (2d Cir. 2017) (citation modified), *overruled on other grounds by Carpenter*, 585 U.S. 296. Given the information available to

CSPD, we conclude that the warrant "[f]ail[ed] to employ the specificity available," making the warrant insufficiently particular. *Leary*, 846 F.2d at 605.

Yet the district court concluded that the affidavit sufficiently narrowed the scope of the warrant to evidence of specific arrests and infractions. *Armendariz*, 2024 WL 2139316, at *11. We think otherwise. As discussed, "the particularity of an affidavit may cure an overbroad warrant" where (1) the affidavit and search warrant are "physically connected," and (2) the search warrant expressly refers to and incorporates the affidavit "using suitable words of reference." *Leary*, 846 F.2d at 603 (citation omitted). The Facebook warrant properly incorporated the affidavit. But the affidavit does little to clarify the scope of the search and seizure. In fact, the affidavit muddies the water by contradicting the warrant's plain language.

The warrant specifically permitted the search of "[a]ll" Facebook posts, Facebook Messenger chats, and Facebook Events. App. vol. I at 120. That term left no ambiguity about the scope of the items sought. *All*, Merriam-Webster, https://www.merriam-webster.com/dictionary/all (last visited Oct. 6, 2025) (defining "all" as, among other things, "the whole amount, quantity, or extent of," "every member or individual component of," and "every"). The warrant's language thus failed to limit the search and seizure to evidence of the identified crimes. *See Leary*, 846 F.2d at 605. Instead, the Facebook warrant allowed officers to search for and seize completely unrelated information. For example, the warrant could have covered Facebook messages as varied as discussions

about other marches to exchanges about favorite dinner recipes. Adopting the officers' position—that the affidavit limited the warrant to evidence of specific crimes—would mean disregarding the word "all" in the warrant itself. That's a leap too far.

As a result, we hold that an affidavit cannot save an insufficiently particularized warrant where the affidavit's language directly contradicts the warrant's language. In those cases, the affidavit does not merely "clarify an ambiguity on the face of the warrant." *United States v. Beaumont*, 972 F.2d 553, 561 (5th Cir. 1992) (emphasis and citation omitted). Instead, the district court reads the affidavit to change the warrant's clear meaning. That type of direct contradiction leaves too much discretion to the executing officers. *See Palms*, 21 F.4th at 698. The Fourth Amendment does not allow officers to choose between conflicting interpretations of the warrant and affidavit.

None of Defendants' other arguments change our minds. Detective Steckler and Sergeant Otero focus on the facts contained in the affidavit and argue that they established probable cause. That argument misses the mark. Sure, the affidavit articulated probable cause for at least some of the information in the broad search-and-seizure categories. But as we have explained, the availability of information to craft a more particularized warrant renders these broad categories deficient. *Leary*, 846 F.2d at 604–05.

The officers also cite various cases to argue against the warrant's overbreadth. None are persuasive. In *United States v. Purcell*, the Second

Circuit upheld a broad warrant that identified twenty-four categories of Facebook data for seizure. 967 F.3d 159, 180–81 (2d Cir. 2020). Importantly, the Second Circuit determined that this broad search satisfied the particularity requirement because the incorporated affidavit made clear that "the suspected criminal activity pervaded [the] entire [Facebook] account." *Id.* at 181 (citation modified). By contrast, the affidavit here never established that the alleged illegality "pervaded" the Chinook Center's Facebook account. The rationale justifying the broad Facebook search in *Purcell* does not apply in this case.

Defendants' reliance on *United States v. Turner*, No. 21-cr-00013, 2022 WL 195083 (D. Nev. Jan. 21, 2022), and *United States v. Liburd*, No. 17-CR-296, 2018 WL 2709199 (E.D.N.Y. June 5, 2018), is similarly misplaced. In both cases, the warrants incorporated affidavits that significantly narrowed the scopes of their respective searches. In *Turner*, the warrant and affidavit "explain[ed] with detail the particular crimes for which evidence was sought and provide[d] objective standards for segregating the responsive material from the non-responsive material." 2022 WL 195083, at *6. And the affidavit listed examples of items for seizure, including Facebook posts, a video showing a false driver's license, and a post with prices for forged documents. *Id.* Similarly, in *Liburd*, the warrant stated that the government "sought to seize information related to the existence of, and communications among, the [criminal organization] and evidence regarding [its crimes]." 2018 WL

2709199, at *2. But here, neither the warrant nor the affidavit narrowed the aims of the search and seizure.

With all this in mind, the Chinook Center plausibly alleged that the Facebook warrant is overbroad.

b. Clearly Established

Because we conclude that the Facebook warrant violates the Fourth Amendment for lack of particularity, we adopt the same clearly-established-law analysis that we applied to the second warrant directed at Armendariz. Contrary to the officers' assertions, we need not point to a case considering a Facebook warrant to find a clearly established right here. *See Mink*, 613 F.3d at 1001 ("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." (citation omitted)). The cases we identified earlier establishing that the second warrant violated clearly established law apply just as well for the warrant targeting the Chinook Center. *See id.* at 1011; *Leary*, 846 F.2d at 602, 605–06; *Voss*, 774 F.2d at 404–05; *Cassady*, 567 F.3d at 636, 643–44.

We therefore reverse the district court's dismissal of the Chinook Center's Fourth Amendment claims against Detective Steckler and Sergeant Otero.

B. Municipal Liability

Plaintiffs also challenge the district court's dismissal of their Fourth Amendment claims against the City. The district court ruled against Plaintiffs on these claims because it determined that Plaintiffs did not allege a plausible Fourth Amendment violation against the City's officers. *Armendariz*, 2024 WL 2139316, at *13.

The district court's reason for dismissing these claims no longer exists. Because we reverse the court's dismissal of the Fourth Amendment claims against the officers, we also reverse the district court's dismissal of these claims against the City. We remand these claims for the district court to determine whether Plaintiffs plausibly alleged municipal liability.

II. Fourth Amendment Injunctive-Relief Claim (Sixth Claim)

Setting aside the search warrants, Armendariz alleged another Fourth Amendment violation—this time against the FBI for retaining her digital data.[17] She argues that the FBI must return or destroy its copies of the digital data that CSPD unlawfully seized from her. But the district court determined that Armendariz did not plead a plausible Fourth Amendment violation, because "[t]he appropriate claim appears to be one for return of property under Fed. R.

[17] Armendariz asserts in a footnote that the district court erred by construing her Fourth Amendment injunctive-relief claim "against only the FBI" and not the City as well. Setting aside that parties waive arguments made only in footnotes, *Griffith v. El Paso County*, 129 F.4th 790, 825 (10th Cir. 2025), the complaint lists the FBI as the only defendant on this claim. As a result, the district court did not err in limiting this claim to the FBI.

Crim. P. 41(g).” *Armendariz*, 2024 WL 2139316, at *15; *see generally* Fed. R. Crim. P. 41(g) (“A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property’s return.”).

Armendariz’s opening brief did not challenge the district court’s rationale for dismissing this claim. “Our law is clear: The first task of an appellant is to explain to us why the district court’s decision was wrong.” *United States v. Martinez*, 92 F.4th 1213, 1265 (10th Cir. 2024) (citation modified); *see also Nixon v. City & Cnty. of Denver*, 784 F.3d 1364, 1366 (10th Cir. 2015) (noting that counsel must “explain what was wrong with the reasoning that the district court relied on in reaching its decision”). Armendariz failed to complete that task.

True, Armendariz argues that the district court erred in dismissing this claim because retaining seized property “can raise independent Fourth Amendment concerns.” Op. Br. at 41. But her opening brief never mentions, let alone challenges, the court’s conclusion that Rule 41 is the proper avenue for relief. So Armendariz waived any argument challenging the district court’s rationale for dismissing this claim. *See Martinez*, 92 F.4th at 1265. We therefore affirm the district court’s ruling without reaching the merits. *See id.*

III. Statutory and State Claims (Third, Fourth, and Fifth Claims)

Finally, Plaintiffs assert that the district court erred by dismissing their Stored Communications Act and state-law claims. They contend that the district

court improperly premised its decision on their failure to allege any constitutional violation.

We agree, with one exception: Armendariz brought an FTCA claim against the United States for an alleged violation of her rights under the Colorado constitution. *See generally* Colo. Const. art. II, §§ 7, 10, 24; Colo. Rev. Stat. § 13-21-131. The district court dismissed this claim because Armendariz failed to plausibly allege that she exhausted administrative procedures under the FTCA. *Armendariz*, 2024 WL 2139316, at *16–17 (citing 28 U.S.C. § 2675(a)). On appeal, Armendariz does not challenge this rationale. Because this waives her argument on that point, we affirm the dismissal of her state-law claim against the United States. *See Martinez*, 92 F.4th at 1265.

On all other claims, Plaintiffs correctly argue for reversal. The district court dismissed the Stored Communications Act claim for the same reasons it dismissed the unlawful-search-and-seizure claims. *See Armendariz*, 2024 WL 2139316, at *14. And after dismissing the federal claims, the court declined to exercise jurisdiction over the remaining state-law claims. *Id.* at *17 (citing 28 U.S.C. § 1367(c)(3)). Because we conclude that Plaintiffs have alleged plausible Fourth Amendment violations, the district court's reasoning no longer applies. So we reverse the dismissal of these claims too.

CONCLUSION

For these reasons, we affirm the district court's dismissal of (1) Armendariz's Fourth Amendment claim for injunctive relief against the

FBI, and (2) Armendariz's state-law claim against the United States. We reverse on all other claims.

No. 24-1201, *Armendariz, et al. v. City of Colorado Springs, et al.*
BACHARACH, J., concurring in part and dissenting in part.

This appeal involves application of the Fourth Amendment to three search warrants for digital devices or their contents. These kinds of warrants might sometimes lack evidentiary support regardless of whether the information is stored in a paper file or in a digital form. An example is the third warrant, where constitutionality turned on established principles of probable cause.

For the other two warrants, however, application of Fourth Amendment principles proved difficult because our case law hadn't kept up with technological advances. *See* David Walker, *Privacy in the Digital Age: Encryption Policy–A Call for Congressional Action*, 1999 Stan. Tech. L. Rev. 3 at *3 ("The courts have historically had difficulty applying the strictures of the Fourth . . . amendment[] to new and emerging technology and have had a tendency to apply existing legal tests created at a time when the new technology was inconceivable."). Without meaningful guidance in the case law, law enforcement officers needed to apply eighteenth-century concepts to the rapidly developing world of digital data. Reasonable officers could differ in how to apply these concepts to the digital devices and their contents.

Reasonable judges could disagree, too. Here, for example, two state judges issued the search warrants and a federal judge concluded that these

warrants had satisfied the Fourth Amendment. Today, however, the majority concludes that those three judges were wrong. Even if the majority is correct, however, the law enforcement officers didn't violate a clearly established right when relying on the approval of two state judges.

Background and Standard of Review

1. This case grew out of searches based on three warrants as the police investigated possible crimes involving a housing protest.

Execution of the three warrants led Ms. Jacqueline Armendariz and the Chinook Center to sue

- four law enforcement officers who had participated in preparing affidavits to support issuance of the warrants,
- the city employing these officers (the City of Colorado Springs), and
- the federal agency (the FBI) that had allegedly retained digital data seized in the searches.

In the suit, Ms. Armendariz and the Chinook Center sued under 42 U.S.C. § 1983, asserting violation of the Fourth Amendment, the Stored Communications Act (18 U.S.C. § 2703 et seq.), and state law. The district court dismissed the federal causes of action for failure to state a claim on which relief could be granted. *See* Fed. R. Civ. P. 12(b)(6).

2. We review the rulings based on the standard for dismissal.

We conduct de novo review over a dismissal for failure to state a valid claim. *Casanova v. Ulibarri*, 595 F.3d 1120, 1124 (10th Cir. 2010).

Conducting this review, we determine whether the complaint stated a plausible basis for relief under 42 U.S.C. § 1983. *Brown v. Montoya*, 662 F.3d 1152, 1162–63 (10th Cir. 2011).

Personal-Capacity Claims Against the Four Officers

1. The personal-capacity claims turn on qualified immunity.

Ms. Armendariz has sued the two officers who participated in obtaining the first two warrants: Detective Daniel Summey and Sergeant Roy Ditzler. And the Chinook Center sued the two officers who participated in seeking the third warrant: Detective B.K. Steckler and Sergeant Jason Otero. The district court dismissed the claims against the four officers based on their defenses of qualified immunity.

To overcome the defense of qualified immunity, Ms. Armendariz and the Chinook Center needed to show the violation of a clearly established constitutional right. *Truman v. Orem City*, 1 F.4th 1227, 1235 (10th Cir. 2021). For purposes of qualified immunity, a right is clearly established if the Supreme Court, the Tenth Circuit, or a consensus of out-of-circuit authority has

- held that "materially similar conduct was unconstitutional" or
- identified a rule that applies "'with obvious clarity'" to the facts.

Buck v. City of Albuquerque, 549 F.3d 1269, 1290 (10th Cir. 2008) (quoting *United States v. Lanier*, 520 U.S. 259, 271 (1997)). A right is clearly

established only if every reasonable law enforcement officer would have realized that the search warrants violated the Fourth Amendment. *Mullenix v. Luna*, 577 U.S. 7, 11–12 (2015).

To assess what every reasonable officer would have realized, we consider the specific circumstances. *E.g.*, *City of Tahlequah v. Bond*, 595 U.S. 9, 12 (2021); *White v. Pauly*, 580 U.S. 73, 79 (2017). The need for specificity is heightened when the alleged violation involves the Fourth Amendment. *D.C. v. Wesby*, 583 U.S. 48, 64 (2018). When the Fourth Amendment is involved, we generally regard a neutral judge's approval of a search warrant as "the clearest indication that the officers acted in an objectively reasonable manner, or in objective good faith." *Messerschmidt v. Millender*, 565 U.S. 535, 546 (2012) (cleaned up). After all, the officers would generally regard the judges as better qualified to apply the Fourth Amendment. *Malley v. Briggs*, 475 U.S. 335, 346 n.9 (1986).

2. Detective Summey and Sergeant Ditzler are entitled to qualified immunity for their roles in obtaining the first two warrants.

a. These warrants grew out of an investigation into interference with a police officer.

The first two warrants grew out of a housing protest by a group called the *Chinook Center*. The attendees included Ms. Armendariz, who walked her bicycle as a police officer tried to arrest one of the protest leaders. Ms. Armendariz dropped her bicycle between herself and the

police officer. The police suspected that Ms. Armendariz had intentionally dropped the bicycle to prevent the officer from catching the protest leader.

The suspicion triggered an investigation of Ms. Armendariz for an attempt to commit aggravated assault against a police officer. The investigation spurred Detective Summey to apply for two search warrants. The first warrant would allow seizure of Ms. Armendariz's digital devices. The second warrant would allow two digital searches:

1. a search of all seized devices for photos, videos, messages, emails, and location data over a period of roughly two months (June 5, 2021, to August 7, 2021) and

2. a key word search for 26 key terms.

Sergeant Ditzler approved both applications, and state judges issued the warrants.

b. First warrant: Seizure of the devices didn't violate a clearly established right.

The issue surrounding the first warrant involves constitutional restrictions when a law enforcement officer seeks digital devices. This issue arises because the warrant allowed the police to enter Ms. Armendariz's residence and seize her cellphones, laptops, external hard drives, and thumb drives.

i. The devices could contain information bearing on Ms. Armendariz's intent.

Ms. Armendariz argues that the devices wouldn't have yielded relevant evidence about the events themselves, pointing out that she had

admittedly dropped the bicycle as a police officer ran toward one of the protest leaders. But the devices could have shed light on Ms. Armendariz's intent: Had she accidentally dropped the bicycle, or had she tried to impede the officer? Given the issue of intent, Detective Summey obtained a warrant to seize Ms. Armendariz's digital devices.

In requesting the warrant, the detective included evidence of Ms. Armendariz's

- active use of social media and
- political involvement.

The detective also relied on his knowledge that people regularly

- attach their phones to computers and use the computers to back up their phones and
- store digital data on numerous devices, including tablets, thumb drives, and external hard drives.

ii. Ms. Armendariz waived her appellate argument about a clearly established violation.

Ms. Armendariz denies probable cause to believe that she

- had relevant information on her devices or
- transferred information from a cellphone to another digital device.

For the sake of argument, we can assume that Ms. Armendariz is right. With this assumption, qualified immunity would turn on whether the Fourth Amendment violation had been clearly established. Ms. Armendariz argues

in her reply brief that the case law clearly established a lack of probable cause to seize a laptop, external thumb drive, or external hard drive. But Ms. Armendariz waived this argument.

In her opening appeal brief, Ms. Armendariz made a general argument involving a clearly established violation. But as to specific deficiencies, Ms. Armendariz addressed only the use of key words in the second warrant. Nowhere in this brief did Ms. Armendariz address the clarity of a violation involving the provisions in the first warrant to allow the seizure of digital devices. She did add this argument in her reply brief, but that was too late. *See WildEarth Guardians v. EPA*, 770 F.3d 919, 933 (10th Cir. 2014). Ms. Armendariz thus waived this argument. *See Campbell v. City of Spencer*, 777 F.3d 1073, 1080 (10th Cir. 2014).

iii. Ms. Armendariz's appellate argument also fails on the merits.

Even if Ms. Armendariz hadn't waived this argument, it would have failed on the merits. The underlying constitutional challenge requires us to ask if there was probable cause to believe that pertinent information existed in a cellphone, laptop, thumb drive, or external hard drive.

Ms. Armendariz questions reliance on Detective Summey's opinion regarding transfers of information between digital devices. For the sake of argument, we can disregard Detective Summey's opinion. Still, however, probable cause could arise from "practical considerations of everyday

life." *United States v. Biglow*, 562 F.3d 1272, 1280 (10th Cir. 2009) (quoting *Anthony v. United States*, 667 F.2d 870, 874 (10th Cir. 1981)).

The resulting question is whether practical considerations of everyday life allow a reasonable inference that Ms. Armendariz transferred digital content among her devices. To answer that question, the issuing judge would have encountered uncertainty because of the nature of the expected information and a dearth of relevant case law.

The probe focused on Ms. Armendariz's possible hostility to law enforcement rather than what she had done. Everyone knew that Ms. Armendariz had impeded a law enforcement officer by dropping her bicycle; the question was why she had dropped the bicycle. Did she drop it by accident or because she wanted to impede the officer?

To investigate that question, Detective Summey requested a warrant for Ms. Armendariz's digital devices.[1] The issuing judge could issue the requested warrant if practical considerations of everyday life created

[1] Ms. Armendariz argues that "it [would have been] unreasonable to believe that a person would incriminate themselves on one device and then transfer that data to every device in her home." Appellants' Opening Br. at 16–17. This argument apparently assumes that the government was seeking evidence of a plan to interfere with the police. But the government was investigating possible hostility to law enforcement, not a plan to interfere with the police. Ms. Armendariz doesn't explain why she would have regarded hostility to the police as incriminating before the housing protest.

probable cause that Ms. Armendariz had transferred pertinent data between her digital devices. *Id.*

In considering these practical considerations, the issuing judge couldn't draw meaningful guidance from precedents because neither our court nor the Supreme Court had addressed the issue. In fact, the only circuit to address the issue (the Fifth Circuit) had rejected a similar challenge to a search warrant for a computer, reasoning that a suspect could have used his cellphone to transfer information to a computer. *United States v. Contreras*, 905 F.3d 853, 859 (5th Cir. 2018).

The majority questions this conclusion based on its perception of typical practices involving the syncing of information among thumb drives and external hard drives. Maj. Op. at 29. But Ms. Armendariz hasn't questioned whether it's common to sync information to these devices. If the majority is right, the resulting question would be whether the practice of syncing information among devices was so antiquated that a police officer should have instantly recognized that no one could reasonably rely on the issuing judge's legal conclusion. *See D.C. v. Wesby*, 583 U.S. 48, 63 (2018). I would answer that question *no* and conclude that any possible violation wouldn't have been clearly established.

The issuing judge implicitly concluded that probable cause existed for seizure of a cellphone, laptop, thumb drive, and external hard drive. In my view, a reasonable officer could competently rely on this resolution of

a debatable question of law. As a result, the alleged violation wouldn't have been clearly established.

iv. The case law didn't clearly establish a requirement for particularized information about the likely presence of multiple devices.

The majority also concludes that the officers violated a clearly established right by assuming that (1) Ms. Armendariz possessed the devices that were listed to be seized and (2) those devices would have the relevant information. Maj. Op. at 27–30. But Ms. Armendariz never made this argument. Absent an argument by Ms. Armendariz, I would decline to reverse on this basis. *See United States v. Tee*, 881 F.3d 1258, 1269 (10th Cir. 2018) (stating that we reverse sua sponte only sparingly and only when exceptional circumstances exist and the parties have obtained an opportunity to address the issue). Even if Ms. Armendariz had made this argument, however, it wouldn't support a clearly established violation.

The affidavit contained evidence of Ms. Armendariz's use of social media and political activism. Together, these statements could lead a reasonable officer to believe that

- Ms. Armendariz had owned a cellphone and
- it would have contained pertinent evidence of her intent.

Would that belief stretch the bounds of reasonableness for purposes of qualified immunity? And does an officer have to provide the same basis for every device sought in a warrant? For this issue, the inquiry would

begin with the case law in existence when the state judge issued the search warrant. *McWilliams v. Dinapoli*, 40 F.4th 1118, 1128 (10th Cir. 2022). But when the search warrant was issued, no meaningful guidance existed in our court or in nine of the other ten regional circuits.

The only regional circuit to address the issue was the D.C. Circuit, which decided *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017). There the court held that a search warrant for digital information was unconstitutional without any information that the homeowner had even owned a digital device. *Id.* at 1272–73. Despite the D.C. Circuit's holding in *Griffith*, we've never based a clearly established constitutional right on a single out-of-circuit opinion. *See Quintana v. Santa Fe Cnty. Bd. of Comm'rs*, 973 F.3d 1022, 1032 n.4 (10th Cir. 2020) (stating that "we cannot endorse the suggestion that one out-of-circuit authority" has created a clearly established right); *see also Avant v. Doke*, 104 F.4th 203, 211 (10th Cir. 2024) (concluding that two out-of-circuit opinions would not create a clearly established right); *Panagoulakos v. Yazzie*, 741 F.3d 1126, 1130–31 (10th Cir. 2013) (concluding that a legal standard adopted by two other circuit courts and two district courts hadn't clearly established the underlying right). Under our past cases, *Griffith* alone wouldn't clearly establish a constitutional requirement for particularized information about the devices likely to be found in Ms. Armendariz's home.

In fact, the D.C. Circuit and other circuits have repeatedly distinguished *Griffith* based on its particular facts. *See United States v. Sueiro*, 59 F.4th 132, 139–41 (D.C. Cir. 2023) (distinguishing *Griffith* when the search warrant included computers and cellphones and the suspect had used some form of "an electronic communications device" to commit the alleged crime); *United States v. Smith*, 108 F.4th 872, 879 (D.C. Cir. 2024) (distinguishing *Griffith* based on evidence that the suspect and victim had used cellphones); *United States v. Vizcarra-Millan*, 15 F.4th 473, 505 (7th Cir. 2021) (distinguishing *Griffith* given the relative weakness of the application for a warrant in that case); *United States v. Davis*, 126 F.4th 610, 616–17 (8th Cir. 2025) (distinguishing *Griffith* because there the application had lacked any evidence involving the use of digital information). In addition, the D.C. Circuit has upheld search warrants after *Griffith*

- for computers and cellphones when the only evidence of a digital device consisted of information including a threat through email, *Sueiro*, 59 F.4th at 139–41 (D.C. Cir. 2023), and
- for cellphones, computers, digital storage devices, and thumb drives when the only evidence involved the use of cellphones and an investigator's experience, *Smith*, 108 F.4th at 878–79.

Even in the D.C. Circuit, then, it's not clear that the court would apply *Griffith* to the search for Ms. Armendariz's digital devices in light of her apparent possession of a cellphone.

Detective Summey obtained the search warrant with sworn statements demonstrating Ms. Armendariz's use of digital devices. These statements involved Ms. Armendariz's

- photos posted by an affiliate of the Chinook Center and
- use of social media to communicate with other protesters.

Detective Summey could reasonably question whether similar statements would have changed the outcome in *Griffith*. So Detective Summey didn't violate a clearly established right even if the issuing judge had lacked probable cause for the presence of multiple digital devices.

c. Second warrant: Authorization of the search and seizure of the contents didn't violate a clearly established right.

The second warrant specified the data that the police could duplicate from Ms. Armendariz's digital devices. The parties disagree over three aspects of the second warrant:

1. The subject-matter
2. The use of key words
3. The historical location data

Limit of the subject-matter

The first aspect involved a reference in the warrant to *this investigation*. Ms. Armendariz characterizes this reference as vague, allowing a search for anything that the officers wanted to view.

The issuing judge disagreed, concluding that the warrant satisfied the Fourth Amendment. We may assume for the sake of argument that

- the issuing judge was wrong and
- the officers shouldn't have relied on the issuing judge's legal conclusion.

Still, Detective Summey and Sergeant Ditzler would enjoy qualified immunity unless every reasonable officer would have realized the inadequacy of the reference to *this investigation*. *D.C. v. Wesby*, 583 U.S. 48, 63 (2018).

The reference to *this investigation* didn't exist in a vacuum: Detective Summey explained that Ms. Armendariz had dropped a bicycle as a police officer ran toward one of the protest leaders. Given this explanation, Detective Summey could reasonably assume that the term *this investigation* referred to the inquiry involving Ms. Armendariz's intent when she dropped her bicycle.

Assume that Detective Summey conducted his own legal research before deciding whether he and Sergeant Ditzler could rely on the warrant. They would have come up empty, as we have, because no precedents existed on the sufficiency of a limit involving relevance to the existing investigation. Given the lack of precedent on this issue, a law enforcement officer could reasonably rely on the warrant's limitation to *this investigation*.

Use of key words

The second disagreement involves the use of key words.

A digital device contains a massive amount of information, and only a fraction would bear on this investigation. For example, investigators would have little use for Ms. Armendariz's digital messages about social engagements and birthdays. So Detective Summey proposed the use of 26 key words to narrow the review of digital information:

> 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, Walls.

Appellants' App'x vol. 1, at 115. Ms. Armendariz argues that the key words didn't adequately constrain the officers. The issuing judge disagreed, concluding that the key words provided a constitutionally sufficient limit on the officers' discretion.

We may again assume that Ms. Armendariz is right and the issuing judge was wrong. Still, Detective Summey and Sergeant Ditzler would enjoy qualified immunity unless every reasonable officer should have realized that the issuing judge had erred in using these key words to constrain the search. *D.C. v. Wesby*, 583 U.S. 48, 63 (2018).

Assume again that Detective Summey and Sergeant Ditzler would have conducted their own legal research to double-check the issuing judge

with respect to the sufficiency of these key words. The detectives would have found two strands of case law.

The first strand consists of Tenth Circuit cases rejecting a rigid requirement for search protocols. *See United States v. Russian*, 848 F.3d 1239, 1245 n.1 (10th Cir. 2017) (stating that "we have previously declined to require a search protocol for computer searches"); *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005) ("This court has never required warrants to contain a particularized computer search strategy."). Other courts had also taken the same approach, rejecting calls for search protocols and *ex ante* restrictions for warrants involving computerized data. Orin Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech L. Rev. 1, 8 (2015).

The second strand of case law approves the use of key words as a way to limit computer searches. *See United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999) (dicta) (discussing key word searches as a way to limit computer searches); *United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir. 2009) (adopting the *Carey* dicta on constraining searches with methods like key word searches).[2]

---

[2] The majority downplays these cases, stating that they refer only to search methodologies while the warrant here permits seizure of the information. Maj. Op. at 42. Ms. Armendariz hasn't drawn this distinction, and we lack briefing on the significance of the wording allowing a *seizure* as well as a *search* of the responsive documents. But even if the majority were right, its distinction crystallizes the difficulty facing the issuing

These two strands of case law reflect the challenge facing law enforcement officers as they applied case law involving conventional searches to the ever-changing world of digital data. The difficulty was magnified with algorithms and cloud technology, creating uncharted challenges for officers seeking relevant information among the limitless data on a typical digital device.

Confronting that challenge, Detective Summey proposed 26 key words to constrain the review of the digital devices. Sergeant Ditzler and the issuing judge approved the key words. If Detective Summey and Sergeant Ditzler had double-checked the issuing judge by doing their own legal research, they would have found little basis in the case law to question the validity of the warrant.

Granted, an error would be obvious if the search warrant had omitted any limiting principles. *See, e.g.*, *Mink v. Knox*, 613 F.3d 995, 1010–11 (10th Cir. 2010) (addressing a warrant that referred only to a general provision permitting the seizure of property that was material to a later criminal prosecution); *Cassady v. Goering*, 567 F.3d 628, 632, 637 (10th Cir. 2009) (addressing a warrant that allowed the search and seizure of "all evidence of any crime"); *United States v. Leary*, 846 F.2d 592, 605–06

---

judge and the officers: They lacked any case law addressing the sufficiency of key words as limits on the seizure of documents appearing on digital devices.

(10th Cir. 1988) (addressing a warrant that covered all communications involving a violation of federal export laws); *Voss v. Bergsgaard*, 774 F.2d 402, 405–06 (10th Cir. 1985) (addressing a warrant that authorized the seizure of any information pertaining to any federal crime). But the search warrant did contain limiting principles through the 26 key words. With these key words, Detective Summey lacked any case law suggesting a failure to adequately constrain the search. Absent such case law, a possible violation of the Fourth Amendment wouldn't have been obvious.

Ms. Armendariz also criticizes some of the key words, invoking a doctrine known as *scrupulous exactitude*. This doctrine could apply when a search warrant targets materials protected by the First Amendment. A classic example arose in *Stanford v. Texas*, 379 U.S. 476 (1965). There officers searched a house and seized over 300 books because they involved suspected connections to the Communist Party of Texas. *Id.* at 477–79. The Supreme Court pointed to a need for "scrupulous exactitude" because the warrant had targeted information protected by the First Amendment. *Id.* at 485.

Ms. Armendariz characterizes the second warrant as authorization of a search targeting protected information. For this characterization, Ms. Armendariz refers to the key words reflecting hostility to the police (such as *pig*, *cop*, and *police*).

The issuing judge rejected this characterization, but we may again assume for the sake of argument that the issuing judge was wrong. With this assumption, qualified immunity would apply unless every reasonable officer should have characterized the key words as code words for information protected by the First Amendment. *D.C. v. Wesby*, 583 U.S. 48, 63 (2018).

Assume again that Detective Summey and Sergeant Ditzler had conducted their own legal research. They again would have come up empty, as we have, because no precedents had addressed the interplay between the First and Fourth Amendments when a warrant targets evidence of hostility toward the police.

Perhaps the issuing judge had erred in overlooking potential parallels to *Stanford*. Even so, obvious differences also existed: There the police targeted information bearing on connections to a communist party because those connections had constituted the underlying crime. *Stanford*, 379 U.S. at 476–77. Here the officers were investigating why Ms. Armendariz had dropped her bicycle: Was it an accident or an effort to impede the police? Answering that question involved intent, and hostility to the police might suggest an intent to impede an officer. *See* Colo. Rev. Stat. § 18-3-203 (stating that intent to cause bodily injury is an element of second-degree assault); *People v. Banks*, 983 P.2d 102, 107 (Colo. App. 1999) (stating that an element of § 18-3-203(c), second-degree assault on a police officer, is

an intent "to cause bodily injury to prevent a police officer from performing a lawful duty").

Ms. Armendariz downplays the difference, and perhaps she's right to do so. But the issuing judge and the officers lacked any meaningful case law on the applicability of *Stanford* when the protected information relates to evidence of intent. Absent meaningful guidance in the case law, a reasonable officer could rely on the issuing judge's legal analysis. So I would reject Ms. Armendariz's reliance on scrupulous exactitude in connection with the search warrant.

Absence of a temporal limitation involving the key words

Despite the use of key words, the warrant didn't include a temporal limitation. Ms. Armendariz argues that the lack of a temporal limitation violated a clearly established constitutional right. For the sake of argument, we can assume that the key words should have contained a temporal limitation. In my view, though, the absence of a temporal limitation didn't render a constitutional violation clearly established.

The key words didn't expand the search—they narrowed it. *See United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999) (dicta) (discussing the use of key words as a way for officers to avoid searching irrelevant material on a digital device); *United States v. Burgess*, 576 F.3d 1078, 1092–93 (10th Cir. 2009) (adopting the *Carey* dicta regarding the use of key words as a method to constrain searches). The digital data contained

a limitless trove of information, and the key words targeted data suggesting hostility to the police.

Ms. Armendariz points out that her act was undisputed: She admittedly dropped her bicycle in the path of an officer running toward one of the protest leaders. So the investigation naturally focused on her intent: Did she accidentally drop the bicycle or try to interfere with an officer? The answer could come from the digital information reflecting Ms. Armendariz's attitude toward the police.

But Ms. Armendariz suggests that the information obviously lost any relevance at some point. We can assume that Ms. Armendariz is right. But neither the Supreme Court nor our court has ever required a temporal limitation on search warrants containing limits involving key words. And one other circuit has resisted efforts to mandate temporal limitations on search warrants for digital data. *See United States v. Zelaya-Veliz*, 94 F.4th 321, 340 (4th Cir. 2024) (declining "to mandate a temporal restriction in every compelled disclosure of social media account data" given the inability to "anticipate all future circumstances").[3] Given the sparsity of pertinent case law, the lack of a temporal limit didn't violate a clearly established right.

---

[3] There the Fourth Circuit declined to require suppression of account data from a social media account, reasoning that the "unsettled nature" of requirements involving temporal limitations would allow an officer with reasonable training to rely on the search warrant. 94 F.4th at 340–41.

Historical data involving Ms. Armendariz's location

The second warrant also allowed officers to seize digital data about Ms. Armendariz's location over a period of roughly two months. She argues that officers had no reason to investigate her whereabouts before the day of the protest. We assume for the sake of argument that Ms. Armendariz is right. But she still had the burden to show that a constitutional violation would have been clearly established. *See* p. 3, above.

On appeal, Ms. Armendariz doesn't argue that a violation would have been clearly established. In her opening brief, she addresses the requirement of a clearly established violation, but only as to the use of key words. For the historical location data, she makes no argument about a clearly established violation. So she has waived that argument. *See Kobach v. U.S. Election Assistance Comm'n*, 772 F.3d 1183, 1192 n.5 (10th Cir. 2014) (stating that an argument is waived when omitted in the appellant's briefs).

3. Detective Steckler and Sergeant Otero are not entitled to qualified immunity for their roles in obtaining the third warrant.

Detective Steckler obtained a third search warrant, which involved the Facebook account for the organization sponsoring the protest (the Chinook Center).[4]

The investigation included potential crimes when protesters allegedly blocked city streets. For this investigation, Detective Steckler requested a warrant identifying

- all subscribers to the Chinook Center's Facebook page and messenger chats,
- Facebook Events, and
- Facebook posts for the four-day period preceding the protest and the two days following the protest.

A state judge approved the warrant, and officers carried out the search. The Chinook Center argues that the warrant obviously failed to establish probable cause for the requested information.

Detective Steckler and Sergeant Otero argue that the search warrant was designed to uncover evidence bearing on plans to block city streets. But Detective Steckler obtained the warrant without presenting any reason to believe that the Facebook materials would include a plan to block the streets.

---

[4] Sergeant Otero approved the application before it was presented to the state judge.

The majority concludes that the warrant was overbroad, Maj. Op. at 49–57, and the Chinook Center argues that we should view the warrant with scrupulous exactitude. In my view, however, we need not address overbreadth or the need for scrupulous exactitude because the warrant lacked any arguable nexus to evidence of a crime.

To obtain the warrant, Detective Steckler presented an affidavit stating that

- the Chinook Center had organized the protest on a Facebook page,
- a tipster had told the police that someone owned a Facebook account with pictures and videos of the protest and the arrest of a protest leader,
- a leader of the protest had posted Facebook messages hostile to the police, and
- a police officer had experience showing that illegal demonstrators use social media to plan events.

The affidavit referred to particular crimes, but didn't say why the Chinook Center's Facebook page would contain information bearing on the blockage of city streets.

The officers argue that the Facebook page could help identify masked protesters.[5] But the affidavit didn't provide a reason to expect information identifying the masked protesters.

Granted, Detective Steckler referred to his experience with the use of social media to plan illegal protests. But the affidavit didn't say why that experience would suggest the presence of digital information bearing on (1) a plan to block the streets or (2) the identification of masked protesters blocking the streets.

Detective Steckler and Sergeant Otero also point out that they lacked meaningful guidance from the case law on Facebook searches. The lack of such guidance could affect the inquiry on overbreadth, but the need for probable cause doesn't turn on the novelty of social media sites like Facebook. For example, suppose that the search warrant had targeted the Chinook Center's paper files rather than a digital site like Facebook. For paper files, Detective Steckler would need a reason to believe that the search would yield evidence of a plan for protesters to block the streets. The same is true for a search warrant targeting a digital site like Facebook.

Despite the relative novelty of Facebook, Detective Steckler provided no reason to believe that the Chinook Center's Facebook account would

---

[5] The officers also say that the Facebook information would bear on a separate prosecution involving one of the protest leaders. But the officers don't develop this statement into a meaningful argument.

reflect planning to block the streets. As a result, the scarcity of case law involving Facebook wouldn't entitle Detective Steckler and Sergeant Otero to qualified immunity for their roles in obtaining the third warrant.

4. The dismissal of state claims should be reversed in light of the majority's conclusion on the federal claims.

The remaining claims against the individual officers arise under Colorado's constitution and laws. Colo. Const. art. II, §§ 7, 10, 24; Colo. Rev. Stat. § 13-21-131. The district court declined to exercise jurisdiction over these claims after dismissing the federal claims.

The majority concludes that Ms. Armendariz and the Chinook Center have alleged plausible federal claims. Based on this conclusion, the majority reverses the dismissal of the state claims against the officers. The reversal is appropriate in light of the majority's conclusions on the federal claims.

Liability of the City Under the First and Fourth Amendments and the Stored Communications Act

Ms. Armendariz and the Chinook Center challenge dismissal of the claims against the City of Colorado Springs for violating the First and Fourth Amendments and the Stored Communications Act (18 U.S.C. § 2703 et seq.). The district court dismissed these claims based on the lack of a constitutional violation, and the majority concludes that municipal employees violated the Constitution in obtaining the three warrants. Given that conclusion, the majority remands for the district court to reconsider

the claims against the city under the First and Fourth Amendments and the Stored Communications Act. This remand is appropriate in light of the majority's conclusion that Ms. Armendariz and the Chinook Center have adequately pleaded constitutional violations.[6]

Claim for Damages Against the Federal Government

Ms. Armendariz also sued the federal government under the Federal Tort Claims Act, seeking damages based on violations of Colorado's constitution and laws. Colo. Const. art. II, §§ 7, 10, 24; Colo. Rev. Stat. § 13-21-131. The district court dismissed these claims, concluding that Ms. Armendariz had failed to satisfy the statutory requirements. The majority concludes that Ms. Armendariz waived her appellate arguments on this claim by failing to challenge the district court's reasoning. Maj. Op. at 60. I agree with the majority and would affirm the dismissal of her claim against the federal government for violating Colorado's constitution and

---

[6] On the claims involving municipal liability, the city argues in the alternative that Ms. Armendariz and the Chinook Center failed to adequately plead an unconstitutional policy or custom. The district court didn't reach this issue, and the preferred approach is to remand for the district court to address this issue in the first instance. *See Rife v. Okla. Dep't of Pub. Safety*, 854 F.3d 637, 649 (10th Cir. 2017); *Greystone Constr., Inc. v. Nat'l Fire & Marine Ins. Co.*, 661 F.3d 1272, 1290 (10th Cir. 2011).

Given this preference, the majority remands for the district court to resolve this issue in the first instance. I agree with this remand in light of the majority's determination that Ms. Armendariz and the Chinook Center adequately pleaded constitutional violations.

laws. *See Nixon v. City & Cnty. of Denver*, 784 F.3d 1364, 1366 (10th Cir. 2015).

Claims Against the FBI for an Injunction

Ms. Armendariz sought an injunction that would require the FBI to return or destroy copies of the digital data obtained in the searches. The district court dismissed this claim, reasoning that (1) a remedy otherwise existed under Federal Rule of Criminal Procedure 41(g) and (2) Ms. Armendariz did not plead a plausible Fourth Amendment violation. The majority correctly upholds this dismissal based on waiver. Maj. Op. at 58–59.

The district court reasoned that Ms. Armendariz and the Chinook Center had an available remedy under Rule 41(g). But Ms. Armendariz and the Chinook Center don't address this reasoning in their opening brief.

They do address this rationale in their reply brief. But the reply brief was too late. *See WildEarth Guardians v. EPA*, 770 F.3d 919, 933 (10th Cir. 2014). Because Ms. Armendariz and the Chinook Center waived their challenge to the district court's reliance on Rule 41(g), I too would affirm the dismissal of this claim. *See Reedy v. Werholz*, 660 F.3d 1270, 1275 (10th Cir. 2011).

Conclusion

The investigations into Ms. Armendariz and the Chinook Center included searches based on three warrants. In my view, Detective Summey

and Sergeant Ditzler enjoyed qualified immunity for their roles in obtaining the first two search warrants. For the third warrant, however, I agree with the majority as to the denial of qualified immunity on the claims against Detective Steckler and Sergeant Otero.

For the claim against the FBI for destruction of the seized data, I believe that Ms. Armendariz and the Chinook Center waived their challenge to the district court's reliance on the availability of another remedy. So I would affirm the grant of the FBI's motion to dismiss.