NO. 24-1201

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

JACQUELINE ARMENDARIZ and CHINOOK CENTER,

PLAINTIFFS-APPELLANTS,

v.

CITY OF COLORADO SPRINGS; DANIEL SUMMEY, a detective with the Colorado Springs Police Department, in his individual capacity; B.K. STECKLER, a detective with the Colorado Springs Police Department, in his individual capacity; JASON S. OTERO, a sergeant with the Colorado Springs Police Department, in his individual capacity; ROY A. DITZLER, a police officer with the Colorado Springs Police Department, in his individual capacity; FEDERAL BUREAU OF INVESTIGATION; and THE UNITED STATES OF AMERICA,

DEFENDANTS-APPELLEES.

On Appeal from the United States District Court
for the District of Colorado - Denver
(Case No. 1:23-CV-01951-SKC-MDB)
Honorable S. Kato Crews, United States District Court Judge

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC PRIVACY INFORMATION CENTER, AND KNIGHT FIRST AMENDMENT INSTITUTE IN SUPPORT OF PLAINTIFFS-APPELLANTS AND REVERSAL

Samir Jain
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K Street, NW, Suite 200
Washington, DC 20005
sjain@cdt.org
(202) 637-9800

Jennifer Lynch
Counsel of Record
Saira Hussain
Brendan Gilligan
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
jlynch@eff.org
(415) 436-9333

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amicus curiae* Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10 percent or more of its stock.

Amicus curiae Center for Democracy & Technology states that it does not have a parent corporation and that no publicly held corporation owns 10 percent or more of its stock.

Amicus curiae Electronic Privacy Information Center states that it does not have a parent corporation and that no publicly held corporation owns 10 percent or more of its stock.

Amicus curiae Knight First Amendment Institute at Columbia University states that it does not have a parent corporation and that no publicly held corporation owns 10 percent or more of its stock.

Dated: August 28, 2024

By: /s/ *Jennifer Lynch*
Jennifer Lynch

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Other Authorities

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization with more than 35,000 dues-paying members. Founded in 1990, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF regularly participates both as direct counsel and as amicus in the Supreme Court, this Court, the Colorado Supreme Court, and other state and federal courts in cases addressing the Fourth Amendment and its application to new technologies. *See*, *e.g.,* *Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014); *Irizarry v. Yehia*, 38 F.4th 1282, 1286 (10th Cir. 2022); *People v. Seymour*, 536 P.3d 1260 (Colo. 2023).

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization that seeks to ensure that the civil rights and civil liberties we enjoy in the physical world are advanced and protected in the digital world. Integral to this work is CDT's representation of the public's interest in protecting individuals from new forms of surveillance that threaten the constitutional and democratic values of privacy and free expression. For over 25 years, CDT has

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), *amici* certify that no party or party's counsel authored this brief in whole or in part, and no person or entity other than *amici*, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief. The parties have consented to the filing of this brief.

advocated in support of laws and policies that protect individuals from unconstitutional government surveillance.

The Electronic Privacy Information Center ("EPIC") is a public-interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC routinely participates as amicus curiae in cases concerning emerging privacy issues, new technologies, and constitutional interests. EPIC has authored many briefs about the constitutional implications of electronic searches. *See, e.g.*, *Carpenter*, 585 U.S. 296; *Riley*, 573 U.S. 373; *Seymour*, 536 P.3d 1260; *O.W. v. Carr*, No. 24-1288 (4th Cir. filed Apr. 8, 2024).

The Knight First Amendment Institute at Columbia University ("Knight Institute" or "Institute") is a non-partisan, not-for-profit organization that works to defend the freedoms of speech and the press in the digital age through strategic litigation, research, and public education. The Institute's aim is to promote a system of free expression that is open and inclusive, that broadens and elevates public discourse, and that fosters creativity, accountability, and effective self-government. Unreasonable searches of electronic devices intrude on personal privacy and burden and chill First Amendment–protected activities. The Institute has a strong interest in ensuring that these searches honor constitutional limits.

INTRODUCTION

The Constitution does not permit law enforcement to use an arrest for a low-level physical offense, combined with allegations based on mere conjecture, to justify dragnet seizures and searches of electronic devices or communications, especially when those searches are aimed at uncovering political speech. But this is exactly what the City of Colorado Springs and its officers ask this Court to accept. Based on little more than unsupported allegations, Appellees sought and received broad warrants authorizing the search and seizure of multiple laptops and cell phones belonging to Ms. Armendariz and a search through a week's worth of data—including private messages—associated with the Chinook Center's Facebook account. These seizures and searches presented an extraordinary invasion of privacy and threatened First Amendment-protected speech.

Given the vast storage capacity of our electronic devices and the varied, personal data they contain, the information available on these devices comprises a "digital record of nearly every aspect of [our] lives." *Riley v. California*, 573 U.S. 373, 375 (2014) . Yet the warrant authorized a virtually limitless search through Ms. Armendariz's devices for her most private records, including every photo, video, message, or email she sent or received over a two-month period and data about everywhere she went during that same time, regardless of whether any of that was in any way related to the crime for which she was charged. The warrant

also authorized a keyword-based search for more than two dozen words—including terms as broad as "celebration," "protest," "housing," "human," and "right." This search had no time limit and therefore could have revealed private information dating back as many years as Ms. Armendariz has kept her data.

Appellees' seizure and search of every private Facebook message the Chinook Center sent or received for a week also gave them access to a wealth of communications—some potentially very revealing—about activists advocating for social and political reform. Not only is the breadth of this seizure and search substantial, it also seems targeted at uncovering disfavored political speech—the very core of what the First Amendment aims to protect.

In the face of this record, the district court erred in granting Appellees' motion to dismiss: Appellants' constitutional rights against the seizures and searches Appellees conducted here were clearly established and Appellees' violation of them cannot be tolerated. This Court should find Appellees are not entitled to qualified immunity, reverse the district court, and allow this case to proceed.

I. ELECTRONIC DEVICES AND SOCIAL MEDIA COMMUNICATIONS CONTAIN AN IMMENSE AMOUNT OF PRIVATE, SENSITIVE DATA

Electronic devices are "a pervasive and insistent part of daily life." *Riley*,

573 U.S. at 385. Ninety percent of Americans own a smartphone.[2] Eighty-one percent own a desktop or laptop computer.[3] Americans access these devices constantly: 89 percent check their phones within ten minutes of waking, and the average American spends over four hours a day looking at their phone.[4]

It should go without saying that our electronic devices contain vast troves of personal data. *Riley*, 573 U.S. at 393, 403 (devices "differ in both a quantitative and a qualitative sense" from other objects because of "all [the personal information] they contain and all they may reveal."). Quantitatively, with their "immense storage capacity," laptops, smartphones, and other electronic devices can contain the equivalent of "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* at 393–94. And this will only grow as electronic devices' storage capacities continue to increase. For example, minimum storage for Apple's

---

[2] Risa Gelles-Watnick, *Americans' Use of Mobile Technology and Home Broadband*, Pew Rsch. Ctr. (Jan. 31, 2024) https://www.pewresearch.org/internet/2024/01/31/americans-use-of-mobile-technology-and-home-broadband/.

[3] *Computer and Internet Use in the United States: 2021*, United States Census Bureau (June 2024), 3, https://www2.census.gov/library/publications/2024/demo/acs-56.pdf.

[4] Alex Kerai, *Cell Phone Usage Statistics: Mornings Are for Notifications*, Reviews.org (Jul. 21, 2023), https://www.reviews.org/mobile/cell-phone-addiction/.

current line of iPhones (128 gigabytes)[5] is eight times greater than that of the top-selling smartphone at the time of the Supreme Court's *Riley* decision. *See* 573 U.S. at 394 (sixteen gigabytes). Apple sells Mac laptops with up to eight terabytes of storage.[6] And customers can purchase external hard drives with up to 100 terabytes of storage.[7]

Given their increasingly immense storage capacities, our devices may contain pictures, communications, location data, and other sensitive records dating back years. This means "even just one type of information [can] convey far more than previously possible." *Riley*, 573 U.S. at 394. For example, access to just the photos on a person's phone allows "[t]he sum of [their] private life [to] be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Id.* Similarly, access to a person's text messages can reveal "a record of all [their] communications" that "can date back to the purchase of the phone, or even earlier." *Id.*

---

[5] *Compare iPhone Models*, Apple (2024), https://www.apple.com/iphone/compare/. 128 gigabytes of storage can store over 26,000 MP3 songs, 36,000 photos, and 20 to 25 high-definition movies. Brent Cohen, *How Much Storage Is 128 GB?*, DeviceTests (Dec. 4, 2022), https://devicetests.com/how-much-storage-is-128-gb.

[6] *See* Jacob Roach, *MacBook Pro M3: Should you choose the M3, M3 Pro, or M3 Max?*, Digital Trends (Nov. 6, 2023), https://www.digitaltrends.com/computing/macbook-pro-m3-buying-guide/.

[7] *ExaDrive*, Nimbus Data, https://nimbusdata.com/products/exadrive/ (last accessed Aug. 25, 2024).

Qualitatively, electronic devices "collect[] in one place many distinct types of information" that "reveal much more in combination than any isolated record." *Id.* Because these devices function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers," and store extensive historical information related to each functionality, they produce and store "digital record[s] of nearly *every* aspect of [users'] lives—from the mundane to the intimate." *Id.* at 393–395 (emphasis added). In turn, this information can "reveal an individual's private interests or concerns," including a person's political affiliations, religious beliefs and practices, sexual and romantic lives, financial status, health conditions, and family and professional associations. *Id.* at 393–96.

Location data, as was sought here, presents its own privacy risks. *See Carpenter v. United States*, 585 U.S. 296, 311 (2018) (noting "time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'") (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). Location data collected directly by a modern cell phone is much more precise than the cell site location data ("CSLI") at issue in *Carpenter*. *Compare Carpenter*, 585 U.S. at 312 (CSLI accurate to within one-eighth to four square miles) *with United States v. Chatrie*, 107 F.4th 319, 349 (4th

Cir. 2024) (noting that data from Google apps on a cell phone "can hunt down a user's whereabouts within meters"). Location data can be collected by (and retrieved from) nearly every app on a user's phone and may be logged "as many as 14,000 times in a single day[,]" even when an app is closed.[8] Location data is also stored in the metadata of images and videos so it can easily be correlated with other data sources to reveal sensitive and private information on where people have traveled, who they were with, and can create inferences about what they might have been doing at the time. *See Riley*, 573 U.S. at 394.

Social media data—also sought here—can reveal sensitive, private information, including First Amendment-protected speech. Americans, including roughly 70 percent of U.S. adults,[9] rely on social media for activities from the everyday to the private and sensitive, *see Packingham v. North Carolina*, 582 U.S. 98, 104–05 (2016), and many rely on its direct messaging features to have private conversations: Facebook estimates that people using its Messenger service send 50 billion messages a day.[10] Activists and organizers also rely on social media and use

[8] Sidney Fussell, *The Most Important Things to Know About Apps That Track Your Location*, Time (Sept. 1, 2022), https://time.com/6209991/apps-collecting-personal-data/.

[9] Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, Pew Rsch. Ctr. (Apr. 7, 2021), https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021.

[10] Nicola Bleu, *27 Latest Facebook Messenger Statistics* (2024 Edition), Blogging Wizard (Jan. 1, 2024), https://bloggingwizard.com/facebook-messenger-statistics/.

messaging services to connect and strategize.[11]

Police can easily download and access all of this sensitive data using mobile device forensic tools. These tools extract "the maximum amount of information possible" from devices, including locally stored data—such as phone contacts, text conversations, photos, videos, saved passwords, GPS location records, and app data.[12] They can even access a person's browser history, previously deleted data, and data stored remotely in the cloud.[13]

Mobile device forensic tools also allow police to analyze the extracted data. For example, they can aggregate data from different apps and sort it by GPS location, file type, or the time and date of creation.[14] Police can then use keywords to search device file names, their contents, or even "across the entire extraction."[15]

---

[11] *See, e.g.*, Samuel Bestvater et al., *Americans' Views of and Experiences with Activism on Social Media*, Pew Rsch. Ctr. (June 29, 2023), https://www.pewresearch.org/internet/2023/06/29/americans-views-of-and-experiences-with-activism-on-social-media/.

[12] Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* (Oct. 2020), 10, 16–17, 21–23, https://perma.cc/7DCK-PGMQ ("Upturn Report").

[13] *See, id. at* 16–17, 21–23. *See also Cellebrite UEFD*, Cellebrite (2023), 102, https://cao-94612.s3.us-west-2.amazonaws.com/documents/Cellebrite_UFED4PC_OverviewGuide_v7.66_July_2023.pdf (discussing File System extraction, which—for unlocked devices—would give access to databases stored on the device that contain users' browsing history).

[14] Upturn Report, *supra* n.12, at 12.

[15] Heather Mahalik, *How To Use the Different Options for Keyword Searching in Cellebrite Physical Analyzer*, Cellebrite (Sept. 5, 2021),

This allows law enforcement to tell a particular story about a person: where they were, what they were doing, when, with whom, and even why. In combination, this can reveal where (and when) someone went to their place of worship or doctor's office, discern every time they ordered takeout, and even identify and map the connections between their friends, family members, acquaintances, and romantic partners. And these tools' capabilities will only continue to grow; for example, one such tool manufacturer, Cellebrite, has begun marketing new AI features for analyzing text, media, web, and financial transaction data extracted from devices.[16]

II. THE WARRANTS WERE OVERBROAD AND LACKED PROBABLE CAUSE AND PARTICULARITY

To prevent every search of a digital device from turning into a general search, warrants must rigorously adhere to the Fourth Amendment's probable cause and particularity requirements, both for the device itself and for the data stored on it. *See generally Riley*, 573 U.S. 373; *United States v. Otero*, 563 F.3d 1127 (10th Cir. 2009). That did not happen in this case. The warrants to seize and search Ms. Armendariz's devices and the Chinook Center's private messages were

---

https://cellebrite.com/en/how-to-use-the-different-options-for-keyword-searching-in-cellebrite-physical-analyzer/.

[16] Ronnen Armon, *AI-Powered Investigations: How Cellebrite is Accelerating Justice with Cutting-Edge Technology*, Cellebrite (Aug. 12, 2024), https://cellebrite.com/en/ai-powered-investigations-how-cellebrite-is-accelerating-justice-with-cutting-edge-technology/.

overbroad and so lacking in probable cause and particularity as to render them invalid. Consequently, their execution violated Ms. Armendariz's and the Chinook Center's constitutional rights.

The Fourth Amendment was enacted to prevent general searches. *Groh v. Ramirez*, 540 U.S. 551, 561 (2004); *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). To accomplish this goal, the Fourth Amendment requires that warrants be supported by probable cause to believe that a crime was committed *and* that evidence of that crime will be found in the place to be searched or the thing to be seized. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Law enforcement must demonstrate "a nexus . . . between the item to be seized and [the] criminal behavior" under investigation. *United States v. Griffin*, 555 F.2d 1323, 1325 (5th Cir. 1977) (quoting *Warden v. Hayden*, 387 U.S. 294, 307 (1967)); *Kohler v. Englade*, 470 F.3d 1104, 1109 (5th Cir. 2006). Warrants must also particularly describe the things to be searched and seized. Through these fundamental limitations, properly drafted warrants prevent overbroad searches and cabin officer discretion.

In this case, the warrants failed to follow constitutionally required limitations. First, the Armendariz warrants failed to show probable cause sufficient to support the seizure and subsequent search of her devices. Even taken in the light most favorable to Appellees, allegations of Ms. Armendariz's actions—throwing

her bicycle in the path of a running officer—do not support probable cause to seize and search electronic devices at all, let alone allow officers to rummage through two months of sensitive and private communications, videos, photos, and location data stored on three cell phones, two computers, and an external hard drive. Nor do these allegations justify a search—without any temporal limitations—through those same devices for over two dozen keywords, many of them commonly used. Second, the Chinook Center warrant also lacked probable cause. The allegations in the affidavit, based on mere conjecture that the Center was involved in organizing an "illegal" march, fail to show that evidence relating to any particular crime would be found in private messages to and from the Center. Finally, even if the Armendariz search warrant were supported by probable cause to believe evidence of the crime would be found on her devices, it was so lacking in particularity as to render it a general search in violation of the Fourth Amendment.

A. Especially in the Context of Digital Searches and Seizures, Warrants Must Be Narrow and Strictly Construed.

Digital devices have the capacity "to store and intermingle a huge array of one's personal papers in a single place." *Otero*, 563 F.3d at 1132. As the Supreme Court recognized in *Riley*, such devices not only "contain in digital form many sensitive records previously found in the home; [but] also contain[] a broad array of private information never found in a home in any form—unless the phone is." *Riley,* 573 U.S. at 396–97. Given this, courts must review warrants to seize or

search digital devices with heightened sensitivity. This supports the "basic purpose" of the Fourth Amendment, which "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Carpenter*, 585 U.S. at 303 (quoting *Camara v. Mun. Ct. of S.F.*, 387 U.S. 523, 528 (1967)). The vast stores of private and sensitive data available on digital devices increase the risk that law enforcement will, after seizing a device, be able "to conduct a wide-ranging search into a person's private affairs," *Otero*, 563 F.3d at 1132, and create "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (*citing United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam)). This risk is especially high where, as here, police seek access to location data *and* attempt to target their search to protected speech. *See Carpenter*, 585 U.S. at 311–312 (recognizing revealing nature of location data); *Tattered Cover v. City of Thornton*, 44 P.3d 1044, 1054–56 (Colo. 2002). To prevent every device search from turning into a general search and to protect device owners' constitutional rights, courts must ensure warrants rigorously adhere to the Fourth Amendment's probable cause and particularity requirements, both for the device itself and for searches of the data stored on it. The district court failed to do so here.

B. Probable Cause to Arrest a Person for Simple Attempted Assault Does Not Automatically Provide Probable Cause to Seize or Search a Device with Vast Amounts of Personal Data.

While the government's allegation that Ms. Armendariz threw her bike at a running officer during a political protest may support an arrest for simple attempted assault, these allegations fail to establish probable cause that her devices would contain evidence related *to the crime charged*: "throw[ing]" her bike. App. Vol. 1 at 92–93.[17] *See United States v. Savoca*, 761 F.2d 292, 297 (6th Cir.) (noting it is "well established" that the "existence of probable cause to arrest will not necessarily establish probable cause to search"). Without this, the warrants to seize and search Ms. Armendariz's devices were invalid.

The officer's bald assertions regarding his experience with white supremacist and hate groups combined with his specious conclusions drawn from internet "research" that Ms. Armendariz associates with communists, App. Vol. 1 at 92, and hates white people, App. Vol. 1 at 102, are not only wholly tangential to the alleged crime, but also fail to provide probable cause to support either the seizure of her devices or such vast and overbroad searches. *See State v. Baldwin*, 664 S.W.3d 122, 135 (Tex. Crim. App. 2022) ("Suspicion and conjecture do not constitute probable cause" to search cell phone); *Gates*, 462 U.S. at 239 ("wholly

[17] Pursuant to Circuit Rule 28.1(A), unless otherwise stated, all record citations are to Plaintiffs-Appellants' Appendix.

conclusory statement" in affidavit is insufficient to support probable cause); *Commonwealth v. White*, 59 N.E.3d 369, 377 (Mass. 2016) ("If [officer's averment that, given the type of crime under investigation, the device likely would contain evidence] were sufficient . . . it would be a rare case where probable cause to charge someone with a crime would not open the person's cellular telephone to seizure and subsequent search"). Despite clear deficiencies in the affidavit, the court below held that it provided probable cause. Were the district court correct, however, police could obtain a warrant to seize and search devices in essentially every case. *See Riley*, 573 U.S. at 399 (only an "inexperienced or unimaginative law enforcement officer . . . could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone"). Such a result would undermine *Riley* and the Supreme Court's recognition that cell phones, "[w]ith all they contain and all they may reveal," hold "the privacies of life." *Id.* at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

Because the warrants to seize and search Ms. Armendariz's devices lacked probable cause, their execution violated her constitutional rights.

C. The Chinook Center Warrant Lacked Probable Cause.

As with the warrants to seize and search Ms. Armendariz's devices, the warrant that authorized search of all private Facebook messages sent and received by the Chinook Center for a week lacked probable cause. *See* App. Vol. 1 at 120.

Private Facebook messages are no different from text messages sent via a cell phone and thus are entitled to the same Fourth Amendment protections. *See, e.g., People v. Herrera*, 357 P.3d 1227, 1234 (Colo. 2015) (recognizing privacy interest in instant messages and need to constrain search); *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017) (recognizing privacy interest in Facebook messages, and consequent need to demonstrate clear probable cause to support search of specific messages).

Here, the Chinook Center was not itself accused of any crime, and the warrant is based on little more than the officer's unsupported assertions that the Center was somehow involved in organizing an "illegal" protest. *See* App. Vol. 1 at 118–19. The Chinook Center "serves as a clearinghouse for progressive activism" and "a community space for existing and emerging organizations and activists to build connections and facilitate projects." App. Vol. 1 at 20. Its website lists more than a dozen such organizations, several of which are involved in issues unrelated to housing justice, the subject of the alleged "illegal" protest.[18] Access to over a week of the Center's private Facebook messages would allow police to map associations within and related to the organization and may well reveal personal information about those who communicated with the Center, such as discussions

[18] *See Member Groups*, Chinook Center, https://www.chinookcenter.org/member-groups (last accessed Aug. 25, 2024).

regarding community issues, political advocacy, and community members' needs. Given the lack of probable cause to support a search of the Center's messages, as well as the privacy interests implicated by an unlawful search, the Chinook Center warrant's execution violated the Center's constitutional rights.

D. The Armendariz Search Warrant Was So Lacking in Particularity as to Constitute a General Warrant.

Even if there were probable cause to support a seizure and limited search of Ms. Armendariz's devices, the search warrant was overbroad and so lacking in particularity that it granted officers "unbridled discretion" to rifle through Ms. Armendariz's most private files and communications, turning the warrant into an unconstitutional general warrant. *Riley*, 573 U.S. at 399 (quoting *Arizona v. Gant*, 556 U.S. 332, 345 (2009)).

The primary function of the Fourth Amendment's particularity requirement is to ensure that government searches are "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). This prevents officers from conducting a "general, exploratory rummaging in a person's belongings." *Coolidge*, 403 U.S. at 467. Search warrants "are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet" of information "to be seized at the discretion of the State."

United States v. Bridges, 344 F.3d 1010, 1016 (9th Cir. 2003). The particularity requirement takes on even greater importance where the property to be searched is a computer or cell phone. *See Otero*, 563 F.3d at 1132 (personal computers' "ability to store and intermingle a huge array of one's personal papers in a single place. . . makes the particularity requirement that much more important").

The Armendariz search warrant embodied this Court's concerns in *Otero*. It allowed officers to rifle through two months of Ms. Armendariz's photos, videos, messages, emails, and location data on six separate devices. App. Vol. 1 at 115. This allowed police to map everywhere she traveled over the course of those two months, whether it was to work, or a friend's house, or her doctor's office—locations completely unrelated to the housing demonstration or the alleged crime. The warrant also allowed officers a virtually limitless search through years of data on those same devices for any appearance or manifestation[19] of 26 keywords—including common words like "assault," "bicycle," "celebration," and several names— regardless of when, how, or in what context they might have been used. App. Vol. 1 at 115. Such broad search criteria could have revealed myriad private details about a person's life, from the most sensitive to the most mundane: such as

[19] Given technological advances, search results from keyword queries on a device are not limited to text. Such queries may also reveal photos or videos, such as an image of a friend's "house" or a video of their birthday "celebration." *See supra* Section I.

a private conversation with a friend about a past sexual "assault," photos of family members on "bicycles," or any reference to or communication with anyone named "Jonathan" or "Samantha"—two of the most common names in the United States.[20] And these details may go back as many years as Ms. Armendariz has kept her data. *See supra* Section I. The search criteria could also have revealed (and, in fact, appear designed to reveal) protected speech. *See infra* Section III. In effect, the warrant authorized police to conduct a digital dragnet in contravention of the Fourth Amendment.

The principle that digital device search warrants are insufficient unless they properly constrain a government search is emphatically reinforced by the Supreme Court in *Riley*. *See* 573 U.S. at 399–401 (discussing concerns with lack of meaningful constraints on government searches). It is also well established by clear precedent in this court and in Colorado state courts. *See Otero*, 563 F.3d at 1132 (collecting cases); *People v. Coke*, 461 P. 3d 508, 516 (Colo. 2020) (warrant to search cell phone that lacked necessary and clear limiting principles "violate[d] the particularity demanded by the Fourth Amendment" and in effect "authorized a general search"); *Herrera*, 357 P.3d at 1230 (government's argument that warrant

[20] *See Top Names Over the Last 100 Years*, Social Security Administration, https://www.ssa.gov/OACT/babynames/decades/century.html (last accessed Aug. 25, 2024) (Jonathan is number 35 for male names, while Samantha is number 40 for female names).

authorized a general search of the entire contents of the phone because evidence could be found anywhere "transforms the warrant into a general warrant that fails to comply with the Fourth Amendment's particularity requirement").

The warrant in this case lacked particularity and failed to properly constrain the government's search. As the Supreme Court recognized in *Groh*, even a search performed pursuant to a warrant, like the search here, can be unconstitutional if the "warrant fails to conform to the particularity requirement of the Fourth Amendment." 540 U.S. at 559 (citing *Stanford v. Texas*, 379 U.S. 476 (1965)). Because the search warrant in this case was overbroad and lacked particularity, it contravened the Fourth Amendment on its face. Therefore, this Court should find that its execution violated Ms. Armendariz's constitutional right to be free from unlawful searches and seizures. And because her rights were "clearly established at the time of the defendant[s'] unlawful conduct," *Est. of Booker v. Gomez*, 745 F.3d 405, 411 (10th Cir. 2014), Appellees are not entitled to qualified immunity, the lower court's judgment should be reversed, and the case should be allowed to proceed.

III. WARRANT REQUIREMENTS MUST BE APPLIED WITH "SCRUPULOUS EXACTITUDE" WHEN EXPRESSIVE RIGHTS ARE IMPLICATED

When a warrant seeks material that is protected by the First Amendment, the requirements of the Fourth Amendment must be applied with "scrupulous

exactitude." *Zurcher v. Stanford Daily,* 436 U.S. 547, 564 (1978) (quoting *Stanford*, 379 U.S. at 485). Appellees' warrants failed to meet this standard both because of the deficiencies in probable cause and particularity, *see supra* Section II, and because the searches clearly were intended to uncover First Amendment-protected activity, including Appellants' political opinions and associations between them and other protesters. For example, one of the search warrants authorized a time-unlimited keyword search of all of Ms. Armendariz's devices for "Chinook Center" and various individuals connected to the Chinook Center, even though there was no indication that the crime police were investigating had any associational component. *See supra* Section II.A. If warrants like the ones in this case are not held to the standards required by the Fourth Amendment, it creates a threat of government officials manipulating warrants to effectively criminalize protected expressive activity, which would disproportionately burden disfavored groups fighting for controversial, and, at times, unpopular causes.

A. Warrants That Fail to Meet Fourth Amendment Requirements Risk Violating Several Constitutional Rights Protected by the First Amendment.

It is "well established" that the First Amendment protects not just the right to free speech, but also "safeguards a wide spectrum of activities, including the right to distribute and sell expressive materials, the right to associate with others, and . . . the right to receive information and ideas." *Tattered Cover*, 44 P.3d at 1051. The

Supreme Court has long recognized the constitutional interests at stake when government officials seize and search expressive material. "[T]he constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain." *Stanford*, 379 U.S. at 485. In situations "[w]here presumptively protected materials are sought to be seized, the warrant requirement should be administered to leave as little as possible to the discretion or whim of the officer in the field." *Zurcher*, 436 U.S. at 564.

In this case, the warrants fell far below this standard. *See supra* Section II. Not only do they lack probable cause or particularity, *id.*, they appear calculated to infringe upon several rights protected by the First Amendment—the right to free speech and expression, the right to freely and privately associate with others, and the right to distribute and receive information.

The Supreme Court has affirmed the "vital relationship between freedom to associate and privacy in one's associations." *NAACP v. Alabama*, 357 U.S. 449, 462 (1958); *see also Bates v. City of Little Rock*, 361 U.S. 516, 523 (1960) (the Constitution guarantees "freedom of association for the purpose of advancing ideas and airing grievances"). The "compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as [other] forms of governmental action." *NAACP*, 357 U.S. at 462.

The Court has also recognized with the advancement of technology, the "most important places . . . for the exchange of views" are "the 'vast democratic forums of the Internet' in general . . . and social media in particular." *Packingham*, 582 U.S. at 104 (quoting *Reno v. ACLU*, 521 U.S. 844, 868 (1997)). Here, the warrants sought to identify associations between Ms. Armendariz and other individuals, including individuals that were not arrested in connection with the protest, but that police believed were connected to the Chinook Center. This included time-unlimited keyword searches that would yield unacceptably broad results of associations beyond the investigation at hand. *See supra* Section II.D. The warrant aimed at the Chinook Center could have uncovered messages from individuals involved in the organization or people interested in becoming involved. *See supra* Section II.C.

Moreover, the Supreme Court repeatedly has held that the right to receive information is a "corollary of the rights of free speech and press" belonging to both speakers and their audience. *Board of Educ. v. Pico*, 457 U.S. 853, 867 (1982) (plurality op.); *see also Kleindienst v. Mandel*, 408 U.S. 753, 762–763 (1972) (cataloging right to receive information in a "variety of contexts"); *Martin v. City of Struthers*, 319 U.S. 141, 146–47 (1943). The right to receive information is also "a necessary predicate to the recipient's meaningful exercise of his *own* rights of speech, press, and political freedom." *Pico*, 457 U.S. at 867 (emphasis added). It is

through listening to others' speech that "our personalities are formed and expressed" and "our convictions and beliefs are influenced, expressed, and tested" so that we can "bring those beliefs to bear on Government and on society." *United States v. Playboy Ent. Grp., Inc*., 529 U.S. 803, 817 (2000). Hence, "[t]he citizen is entitled to seek out or reject certain ideas or influences without Government interference or control." *Id.*; *Stanley v. Georgia*, 394 U.S. 557, 565 (1969).

In this vein, the Colorado Supreme Court has articulated an even higher standard for warrants seeking to uncover people's interest in specific reading material. In *Tattered Cover*, police obtained a warrant to search a bookstore's records for a suspect's transaction history, and the bookstore filed suit to restrain officers from executing it. 44 P.3d at 1050. The court held that because the state constitution "provides more expansive protection of speech rights than provided by the First Amendment," a warrant seeking to discover a person's interest in specific reading material required a higher standard than just probable cause. *Id.* at 1054–56.

Here, the broad searches authorized in the Armendariz and Chinook Center warrants implicate both materials that Appellants may have sent to others and ideas and information they may have received from others. In addition, time-unlimited searches for keywords such as "housing" and "protest" could uncover vast swaths of information—not just text messages, emails, photos, and videos, but also results

from the device owner's browser search history. *See supra* Section I. As with reading lists, disclosure of users' search queries chills their right to seek out information and deters participation in the "uninhibited, robust, and wide-open debate and discussion" contemplated by the First Amendment. *See Lamont v. Postmaster Gen. of U.S.*, 381 U.S. 301, 307 (1965); *see also Tattered Cover*, 44 P.3d at 1055–56.

B. Warrants That Fail to Meet Fourth Amendment Requirements Disproportionately Burden Disfavored Groups.

The principle that warrants meet Fourth Amendment requirements with "scrupulous exactitude" is especially important to protect the rights of disfavored groups, including organizations fighting for social and economic justice such as the Chinook Center and its fourteen member organizations.[21] *Stanford*, 379 U.S. at 485.

Cases like this one at the intersection of expressive freedoms and government searches directly motivated the Framers' disapproval of general warrants and the adoption of the Fourth Amendment. Discussing the British "use of general warrants as instruments of oppression," the Supreme Court noted that "this history is largely a history of conflict between the Crown and the press." *Id.* at 482. The Court went on further to recognize that "[t]he bill of Rights was

[21] *See supra* n.18.

fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression." *Id.* at 484. Examination of the warrants in this case reveal that Appellants' speech and other expressive activities appear to have been a motivating factor for their arrests and the subsequent seizure and search of their devices and Facebook messages.

The affidavits in support of the Armendariz and Chinook Center search warrants are littered with references to protected speech and speculations about what that speech could mean. For example, in the Armendariz warrant, the officer noted that some protesters "carried red flags," editorializing that they were "a radical political symbol" associated with "socialism and communism" that "designate[] this march…as revolutionary and radical in nature." App. Vol. 1 at 92. The affidavit further extrapolated that Ms. Armendariz's use of "yt" in a social media profile "show[ed] her disdain for white people." App. Vol. 1 at 102. Likewise, the Chinook Center warrant affidavit described that the purported leader of the Chinook Center, Shaun Walls, "extended his middle finger toward the police line" immediately before a lieutenant ordered his arrest.[22] *See* App. Vol. 1 at 118. Both warrants extensively detailed social media posts by Mr. Walls expressing his

[22] At least two federal appellate courts have held that a raised middle finger cannot constitute reasonable suspicion or probable cause for a stop, let alone an arrest. *Cruise-Guylas v. Minard*, 918 F.3d 494, 496 (6th Cir. 2019); *Wilson v. Martin*, 549 F. App'x 309, 311 (6th Cir. 2013); *Swartz v. Insogna*, 704 F.3d 105, 110 (2d Cir. 2013).

political opinions—and notably, neither affidavit claimed the speech constituted true threats or was otherwise unprotected. Yet, these posts formed the basis for probable cause to search by keyword for associations with Ms. Armendariz and through the Chinook Center's Facebook information and communications.

This specious basis for searches of vast amounts of digital information is especially problematic when considering that laws governing mass assemblies offer officers extensive discretion. "[L]aw enforcement routinely uses low-level criminal law," such as charges of unlawful assembly, obstructing traffic, and resisting arrest "to manage the disruptiveness of protests, with judicial approval." Tabatha Abu El-Haj, *Defining Peaceably: Policing the Line Between Constitutionally Protected Protest and Unlawful Assembly*, 80 Mo. L. Rev. 961, 964 (2015). For example, unlawful assembly ordinances only require that "participants are at some point planning to engage in forceful or violent lawbreaking," and allow officers ample discretion to determine when that threshold has been met. John Inazu, *Unlawful Assembly as Social Control*, 64 UCLA L. Rev. 2, 7 (2017). Police have relied on unlawful assembly ordinances to target "civil rights workers, antiabortion demonstrators, labor organizers, environmental groups, Tea Party activists, Occupy protesters, and antiwar protesters." *Id.* at 5. Here, police used Colorado Springs' analogous ordinance—"obstructing passage or assembly," which makes "unlawful" many acts associated with a protest, such

as blocking a roadway or "[d]isobey[ing] a reasonable request or order to move issued by a person known to be a peace officer"[23]—to arrest Mr. Walls and other prominent Chinook Center members even *after* they complied with requests to move onto the sidewalk. App. Vol. 1 at 18, 27. As scholars have noted, "the fact that state courts would be likely to dismiss charges or overturn convictions" for such low-level offenses "provides little comfort" because "[s]uch arrests take protesters off the streets, rendering their formal constitutional rights meaningless." Abu El-Haj, *supra*, at 974. This injustice is compounded if officers are authorized virtually unfettered access to a protester's electronic devices under the guise of further investigating that low-level offense. *See supra* Section II.B.

Courts should not allow government officials seeking to chill speech the ability to rifle carte blanche through critics' private data. Warrants that purport to authorize such actions, like those at issue in this case, are plainly unconstitutional.

CONCLUSION

For the reasons stated above, Appellants have sufficiently pled that the Armendariz and Chinook Center warrants failed to meet the Fourth Amendment requirements of probable cause and particularity. This Court should reverse the district court's dismissal and allow the case to proceed.

[23] Colo. Springs Ord. § 9.2.104.

Dated: August 28, 2024

Respectfully submitted,

/s/ *Jennifer Lynch*

Jennifer Lynch

Saira Hussain
Brendan Gilligan
Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
jlynch@eff.org
(415) 436-9333

Samir Jain
Center for Democracy & Technology
1401 K Street, NW, Suite 200
Washington, DC 20005
sjain@cdt.org
(202) 637-9800

Attorneys for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g)(1)I certify as follows:

1. This Brief of Amici Curiae Electronic Frontier Foundation, Center for Democracy & Technology, Electronic Privacy Information Center, and Knight First Amendment Institute, with the type-volume limitation of Fed. R. App. P. 29(a)(5) because this brief contains 6,482 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and Circuit Rule 32(A) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, the word processing system used to prepare the brief, in 14-point font in Times New Roman font.

Dated: August 28, 2024

/s/ *Jennifer Lynch*
Jennifer Lynch

CERTIFICATE OF DIGITAL SUBMISSION

I hereby certify that with respect to the foregoing:

(1) all required privacy redactions have been made per 10th Cir. R. 25.5;

(2) if required to file additional hard copies, that the ECF submission is an exact copy of those documents;

(3) the digital submissions have been scanned for viruses with the most recent version of a commercial virus-scanning program, Virus Total, updated August 27, 2024, and according to the program are free of viruses.

Dated: August 28, 2024

/s/ *Jennifer Lynch*
Jennifer Lynch

CERTIFICATE OF SERVICE

I certify that on August 28, 2024, I electronically filed the foregoing Brief of Amici Curiae using the Court's CM/ECF system which will send notification of such filing to all parties of record.

Dated: August 28, 2024

/s/ *Jennifer Lynch*
Jennifer Lynch