THOMAS C. SEABAUGH (SBN 272458)
tseabaugh@seabaughfirm.com
LAW OFFICE OF THOMAS C. SEABAUGH
355 S. Grand Ave., Suite 2450, Los Angeles, CA 90071
Telephone: (213) 225-5850

RACHEL LEDERMAN (SBN 130192)
rachel.lederman@justiceonline.org
PARTNERSHIP FOR CIVIL JUSTICE FUND, & its project
THE CENTER FOR PROTEST LAW & LITIGATION
1720 Broadway, Suite 430, Oakland, CA 94612
Telephone: (415) 508-4955

CHESSIE THACHER (SBN 296767)
cthacher@aclunc.org
SHAILA NATHU (SBN 314203)
snathu@aclunc.org
ANGELICA SALCEDA (SBN 296152)
asalceda@aclunc.org
ACLU FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street, San Francisco, CA 94111
Telephone: (415) 621-2493

*Attorneys for Plaintiffs*

**SUPERIOR COURT OF THE STATE OF CALIFORNIA**
**COUNTY OF SANTA CRUZ**

HANNAH (ELIO) ELLUTZI; LAAILA IRSHAD; CHRISTINE HONG,

Plaintiffs,

vs.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA; CYNTHIA LARIVE, in her official capacity as Chancellor of the University of California, Santa Cruz ("UCSC"); LORI KLETZER, in her official capacity as UCSC Campus Provost and Executive Vice Chancellor; EDWARD D. REISKIN, in his official capacity as UCSC Vice Chancellor for Finance, Operations and Administration; AKIRAH J. BRADLEY-ARMSTRONG, in her official capacity as UCSC Vice Chancellor of Student Affairs; ALEX DOUGLAS MCCAFFERTY, in his official capacity as UCSC Campus Budget Director; SONYA KIERNAN, in her official capacity as Executive Assistant to the UCSC Chancellor; HERBERT LEE, in his official capacity as UCSC Vice Provost of Academic

Case No. 24CV02532
*Assigned for all purposes to the Hon. Syda Kosofsky Cogliati*

**MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF PLAINTIFF LAAILA IRSHAD'S MOTION TO QUASH, VOID, OR MODIFY SEARCH WARRANT RE: DISCOVERY OF ELECTRONIC INFORMATION**

**(Pen. Code, § 1546.4(c))**

**Date:** December 19, 2024
**Time:** 8:30 a.m.
**Dept.:** 5

Action Filed: September 9, 2024

*[Filed concurrently with Notice of Motion and Motion to Quash, Void, or Modify Search Warrant Re: Discovery of Electronic Information]*

Affairs; JESSICA RASHID, in her official capacity as UCSC Assistant Dean of Students, Student Conduct & Community Standards; ADRIENNE RATNER, in her official capacity as UCSC Director of Academic Employee Relations; KEVIN DOMBY, in his official capacity as UCSC Chief of Police and Executive Director of Public Safety; and DOES 1-10,

Defendants.

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Statutes** ..... **Page(s)**



**Rules** ..... **Page(s)**



**Other Authorities** ..... **Page(s)**

## MEMORANDUM OF POINTS AND AUTHORITIES

### I. INTRODUCTION

By this Motion, Plaintiff Laaila Irshad respectfully petitions the Court for an order quashing, voiding, or modifying the search warrant for her cellphone issued on September 25, 2024. Ms. Irshad brings this motion pursuant to the California Electronic Communications Privacy Act (CalECPA), Penal Code section 1546 *et seq.* Specifically, subsection (c) of Section 1546.4 authorizes individuals such as Ms. Irshad—"whose information is targeted by a warrant . . . that is inconsistent with [CalECPA], or the California Constitution or the United States Constitution"—to file a petition "to void or modify the warrant, order, or process, or to order the destruction" of unlawfully obtained information. The warrant here is largely unbounded as to time and scope, and lacks the particularity required by law. It sweeps in an enormous range of Ms. Irshad's private and sensitive information, including attorney-client privileged communications and attorney work product related to this action. It also smacks of retaliation given that officers at the University of California Santa Cruz (UCSC) sought this warrant a little more than two weeks after Ms. Irshad initiated the present action alleging that they had engaged in unconstitutional conduct. Because the warrant violates CalECPA, the First and Fourth Amendments, and the California Constitution, it should be quashed, voided or, at a minimum, modified.[1]

### II. STATEMENT OF FACTS

#### A. Laaila Irshad's Role as Plaintiff

Ms. Irshad is a third-year undergraduate student and Resident Advisor (RA) at UCSC. (Decl. of Laaila Irshad in Support of Mot. to Quash, ¶ 2.) On September 9, 2024, Ms. Irshad commenced the present civil rights action with two other plaintiffs to challenge the

[1] Ms. Irshad recognizes that, under Penal Code section 1546.4(c), there is a presumption that any petition to quash, void, or modify be heard by the magistrate judge who issued the challenged warrant. The Clerk's Office has, however, advised counsel for Ms. Irshad that such a petition or motion to quash cannot be filed before the magistrate as no criminal charges have been filed. Given the urgency of the issues raised herein, Ms. Irshad cannot wait to see if such charges will be filed. Therefore, Ms. Irshad seeks to petition this Court for relief. If the Court determines that this petition should ultimately be heard by the issuing magistrate, Ms. Irshad has no objection to the transfer of this particular matter to a different department.

unconstitutional summary banishment of protesting students and faculty at the end of May 2024. The lawsuit named, among other defendants, Chief Kevin Domby, in his official capacity as UCSC Chief of Police and Executive Director of Public Safety.

A little more than two weeks after Ms. Irshad filed her lawsuit accusing Chief Domby and UCSC police officers of unconstitutional conduct and due process violations, a member of the UCSC Police Department—Detective James Watson—sought a warrant authorizing the seizure and search of Ms. Irshad's cellphone. (Irshad Decl., Ex. A.) The warrant was issued on September 25, and UCSC officers served it on October 1—just five days after Plaintiffs had filed a Motion for Preliminary Injunction including a declaration submitted by Ms. Irshad. (*Id.*, ¶¶ 3-5.)

**B. Execution of Search Warrant on Laaila Irshad**

In the early morning of October 1, 2024, Ms. Irshad was in her on-campus apartment when a fire alarm sounded. (Irshad Decl., ¶ 3.) Because she was an RA, Ms. Irshad, still dressed in her pajamas, knocked on doors to alert students of the alarm and then guided them out of the building. (*Ibid.*) Once outside, she gathered with about 400 students in a nearby field to await further instructions. (*Ibid.*) While she was in the field, UCSC police officers approached, served her with a search warrant, and took her cellphone. (*Id.*, ¶ 4.) It was a very public and embarrassing encounter that left Ms. Irshad with the impression that she was being singled out for punishment.

In particular, the warrant included a screenshot picture of Ms. Irshad being interviewed by KSBW Action News 8 about the filing of the present case. (*Id.*, ¶ 5.) Accompanying the news segment was an article entitled "UC Santa Cruz Faces Lawsuit Over Handling of Campus Protests." (*Ibid.*) UCSC officers used this screenshot picture of Ms. Irshad notwithstanding that the school had access to her student ID photo—thus reinforcing her belief that she was being punished for having participated in this civil rights action. (*Ibid.*)

Since UCSC police officers seized her cellphone, Ms. Irshad has experienced significant hardships. (*Id.*, ¶¶ 6-11.) Her phone, like the phones of most people, holds the intimate details of life—Ms. Irshad's personal information, contacts and telephone numbers, internet search caches, pictures of friends and family, banking accounts, medical information, and many intensely private emails and text messages. (*Id.*, ¶ 7.) Her phone also contains emails, voicemails, and text messages

exchanged with attorneys discussing legal advice, including communications with undersigned counsel about this case. (*Id.*, ¶ 8.) Without her phone, Ms. Irshad has had difficulty finding a secure way to talk with her legal team. (*Ibid.*)

Additionally, because so many of UCSC's systems require a phone-based dual-authentication process, Ms. Irshad has struggled to access her UCSC email and student portal, and to complete class assignments on the portal. (*Id.* ¶ 9.) She has also struggled because certain apps on her phone are necessary for her RA responsibilities. (*Id.* ¶ 10.) It has even been difficult for Ms. Irshad to do her laundry because the campus machines operate by scanning QR codes for payment. (*Ibid.*) Ms. Irshad does not have funds sufficient to purchase a phone on her own and both the disruption and financial burden of having her phone seized have been significant. (*Id.*, ¶¶ 9, 11.)

**C. Overbroad Scope of Search Authorized by Warrant**

The Search Warrant issued on September 25, 2024 authorizes the police to search "[a]ll data constituting evidence and instrumentalities of Penal Code section 594(a) vandalism, including communications referring or relating to the above-listed criminal offenses, between **date of inception of first data storage in the device(s) to the date of warrant execution"** including:

> **a. All communications content**, including email, text (short message service (SMS)/ multimedia message service (MMS) or application chats), notes, or voicemail. This data will also include attachments, source and destination addresses and time and date information, and connection logs, images and any other records that constitute evidence and instrumentalities of Penal Code Section 594(a) Vandalism, including communications referring or relating to the above-listed criminal offenses, together with indicia of use, ownership, possession, or control of such communications or information found.
>
> **b. All location data.** Location data may be stored as GPS locations or cellular tower connection data. Location data may be found in the metadata of photos and social networking posts, Wi-Fi logs, and data associated with installed applications.
>
> **c. All photographic/video/audio data** and associated metadata.
>
> **d. All internet history**, including cookies, bookmarks, web history, search terms.
>
> **e. All indicia of ownership** and control for both the data and the cellular device, such as device identification and settings data, address book/contacts, social network posts/ updates/tags, Wi-Fi network tables, associated wireless devices (such as known Wi-Fi networks and Bluetooth devices), associated connected devices (such as for backup and syncing), stored passwords, user dictionaries.

(Irshad Decl., Ex. A, emphasis in original.)

## III. ARGUMENT

Because Ms. Irshad has access to only an excerpted copy of the search warrant and is currently unable to review the sealed affidavit in support, this Motion does not address whether probable cause exists to justify a targeted search of Ms. Irshad's cellphone. Rather, this Motion focuses on deficiencies of particularity and proceeds in four parts: ***First***, the Motion sets forth the governing CalECPA statutory framework; ***Second***, the Motion explains why the search warrant's overbreadth violates CalECPA, as well as federal and state constitutional law; ***Third***, the Motion establishes that the search warrant risks compromising attorney work product and attorney-client privileged communications; and ***Finally***, this Motion argues that the Court should consider unsealing the affidavit.

### A. CalECPA Provides Robust and Mandatory Protections Where, As Here, Digital Privacy is at Stake

#### 1. Heightened Particularity Requirement

A decade ago, the United States Supreme Court in *Riley v. California* (2014) 573 U.S. 373 (*Riley*) recognized that today's digital devices contain vast amounts of extremely sensitive, private information. The *Riley* Court observed: "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" (*Id.* at pp. 396, 403, citation omitted.)

Following *Riley*, the Legislature enacted CalECPA, Penal Code section 1546 *et seq.*, to modernize California's privacy protections in the digital age. The Act establishes two important safeguards to protect Californians' privacy rights when electronic communications and device information are the subject of a search. These rules go beyond those present in federal law.[2]

[2] *See* Nicole Ozer, *California is Winning the Digital Privacy Fight* (Nov. 7, 2015) Tech Crunch, <https://techcrunch.com/2015/11/07/california-now-has-the-strongest-digital-privacy-law-in-the-us-heres-why-that-matters/> [as of Oct. 11, 2024]; Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law* (Oct. 8, 2015) Wired, (quoting CA State Senator Mark Leno) <https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/> [as of Oct. 11, 2024].

First, CalECPA protects all "electronic device information" and all "electronic communications information" from government access, no matter the source or nature of that information. (*See* Pen. Code, § 1546, subd. (d) [definition of "electronic communication information"]; *id.*, § 1546, subd. (g) [definition of "electronic device information"]; *id.*, § 1546.1, subd. (a)(1)–(3) [protecting both electronic communication and device information].) And second, CalECPA requires that any warrant seeking access to electronic information be highly specific and narrowly cabined. The statute mandates that a search warrant "***describe with particularity*** the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought . . . ." (Pen. Code, § 1546.1, subd. (d)(l), emphasis added.)

CalECPA's heightened particularity requirement is a direct response to the concern in *Riley* that government officials do not get a free-for-all when searching the "vast quantities of personal information" on our digital devices. (*Riley*, *supra*, 573 U.S. at p. 386.) The Supreme Court reinforced this understanding in *Carpenter v. United States* (2018) 585 U.S. 296, noting that a "cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." (*Id.* at p. 311.) California courts are similarly in accord because there is no question that a cellphone search "could potentially expose a large volume of documents or data, much of which may have nothing to do with illegal activity." (*People v. Appleton* (2016) 245 Cal.App.4th 717, 725.) Such documents or data might "include, for example, medical records, financial records, personal diaries, and intimate correspondence with family and friends." (*Ibid.*)

**2. Explicit Remedies for any CalECPA Violation**

One prominent feature of CalECPA's statutory privacy framework are the remedies available for violations of CalECPA, as well as for violations of the California and United States Constitutions. These remedies reflect that the Legislature understood the implications of robust judicial enforcement to address a violation of law, including suppression of evidence, the invalidation of search warrants, and the wholesale deletion of unlawfully obtained material.

Specifically, the statute provides that, if a search warrant is "inconsistent with" CalECPA or the California or United States Constitutions, the targeted individual may petition the court to void or modify the warrant, or to order the destruction of any improperly obtained data or information. (Pen. Code, § 1546.4, subd. (c).) That CalECPA authorizes voiding a warrant and the destruction of evidence is an important feature of the statutory scheme—and one that required CalECPA to pass the California Legislature by a supermajority vote.[3] CalECPA's authors highlighted the importance of this suppression remedy as the best way to ensure compliance with the statute's rules.[4]

Alternatively, a court may appoint a "special master" to ensure that "only information necessary to achieve the objective of the warrant . . . is produced or accessed." (*Id.*, § 1546.1, subd. (e)(1).) These provisions reflect that the Legislature recognized two important characteristics of digital-age information: that people who communicate with the target of a warrant can have their privacy invaded by overbroad or unlawful warrants; and that the *mere possession* of information by the government (even if it is locked away) has the potential to cause harm. (*See Sanchez v. Los Angeles Dept. of Transportation* (9th Cir. 2022) 39 F.4th 548 [holding that retention of records alone is sufficient to establish Article III standing].)

### B. The Search Warrant is Overbroad in Violation of CalECPA, the Fourth Amendment, the First Amendment, and the California Constitution

#### 1. The Warrant fails to satisfy CalECPA's and the Fourth Amendment's particularity requirements.

Similar to CalECPA, the Fourth Amendment also mandates that a warrant "***particularly describe*** the place to be searched, and the persons or things to be seized." (*Groh v. Ramirez* (2004)

---

[3] *See* Cal. Const., art. I, § 28, subd.(d). The two-thirds majority was only necessary for CalECPA because the law mandates suppression of information *beyond* that which is required by the United States Constitution. (*In re Lance W.* (1985) 37 Cal.3d 873, 879). If CalECPA had included just the suppression mandated under federal law, a simple majority would have been sufficient.

[4] Summary of the California Electronic Communications Privacy Act, Senators Leno and Anderson (Sept. 2, 2015) <https://www.aclunc.org/sites/default/files/SB%20178%20CalECPA%20Fact%20Sheet_1.pdf> [as of Oct. 11, 2024]. *See also Elkins v. United States* (1960) 364 U.S. 206, 217 [noting that the purpose of suppression "is to deter—to compel respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard it"].

540 U.S. 551, 557 [emphasis added, internal quotation omitted].) The same standard inheres in the California Constitution. (Cal. Const., art. I, § 13.) The "manifest purpose of this particularity requirement" is "to prevent general searches." (*DiMaggio v. Super. Ct. of Monterey County* (2024) 104 Cal.App.5th 875, 887 [citing *Maryland v. Garrison* (1987) 480 U.S. 79, 84].) "By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." (*Ibid.*) Said another way: the Constitution prohibits "general warrants" that would allow the government to "rummage" through someone's personal effects. (*Coolidge v. New Hampshire* (1971) 403 U.S. 443, 467.)

In determining whether a warrant is overbroad, courts consider whether probable cause existed to seize all items of a category described in the warrant and if the government could have provided more particularity based on information available. "'[G]eneric classifications in a warrant are acceptable only when a more precise description is not possible.'" (*U.S. v. Kow* (9th Cir. 1995) 58 F.3d 423, 427) [quoting *U.S. v. Cardwell* (9th Cir. 1982) 680 F.2d 75, 78].) In *People v. Meza* (2023) 312 Cal.Rptr.3d 1, for example, the court found portions of the warrant overbroad where, *inter alia*, the timeframe was not narrowly tailored given the information available. (*Id.* at p. 18; *see also Kow, supra,* 58 F.3d 423 at p. 427 [warrant not sufficiently particular where it did not limit scope of seizure to a time frame within which suspected criminal activity took place].)

The search warrant at issue here flies in the face of this longstanding law. It seeks virtually ***all*** data stored on Ms. Irshad's personal cellphone from the "date of inception of first data storage in the device(s) to the date of warrant execution." (Irshad Decl., Ex. A.) And it demands access to "all communications content," "all location data," "all photographic/ video/ audio data," "all internet history," and "all indicia of ownership." It is hard to reconcile how such a broad search could be tethered to the investigation of an alleged act of vandalism.

The search warrant's time frame is both meaningless and all encompassing. Presumably UCSC knows the date, or date range, that the alleged act of vandalism occurred. But by pegging

the start of the search on an unknown date (i.e., whenever the phone was activated) and by failing to address how data imported from any of Ms. Irshad's prior digital devices should be treated, the warrant threatens to capture the complete history of Ms. Irshad's digital life.[5] Moreover, the time period from when Ms. Irshad first began using her cellphone, to the present, almost certainly predates any incident UCSC police might be investigating—and perhaps even predates her time as a student at UCSC. There is simply no legitimate reason for UCSC officers to "rummage" through everything on Ms. Irshad's phone from its first use to the present.

The warrant's scope is similarly unrestricted. As discussed *supra*, law enforcement access to digital material on a seized cellphone is profoundly invasive and therefore should be narrowly cabined. Not so here. The warrant authorizes a search of everything from Ms. Irshad's internet browsing history to her texts with family to the metadata on every one of her photographs. As soon as an officer views these photographs and other material during the execution of a search, privacy interests are "compromised." (*Appleton*, *supra*, 245 Cal.App.4th at pp. 725–726.)

Worse yet, an overly broad search of one person's device also implicates the privacy interests of third parties who interact with that person. (*See In re Malik J.* (2015) 240 Cal.App.4th 896, 903.) For this reason, "it is the constitutionally imposed duty of the government to carefully tailor its search parameters to minimize infringement on the privacy rights of third parties." (*Meza*, *supra*, 312 Cal.Rptr.3d at p. 18 [citation omitted].) The government has not discharged that duty faithfully here. Because the warrant in this case fails to restrict the time period or describe with sufficient particularity the items to be seized, it is indistinguishable from the general warrants repeatedly held to be unconstitutional. Under CalECPA, the Fourth Amenment, and the California Constitution, these failures call for the Court's swift intervention.

[5] The warrant could reach information stored after the device was initialized—but originating even farther back in time—because many people's first step when they acquire a new device is to transfer all the information from a previous device (whether directly or from backup). And so a great deal of information, from photos to documents to communications with others, can be added to a new device during the "activation" process.

**2. The Warrant infringes Ms. Irshad's rights to free speech, free expression, and free association.**

In addition to implicating her rights under the CalECPA, the Fourth Amendment, and the California Constitution, the search of Ms. Irshad's phone impermissibly encroaches on Ms. Irshad's rights to free speech, free expression, and free association protected by the First Amendment and Article I, sections 2 and 3, of the California Constitution. It poses the same threat to any person who communicated or interacted with Ms. Irshad on her cellphone.

**a. Retaliatory Search and Seizure**

Both the U.S. and California Constitutions protect the right to petition government officials and to access the courts free from retaliation, including retaliatory investigative or enforcement actions. (*See, e.g.*, *Woodruff v. Mason* (7th Cir. 2008) 542 F.3d 545, 547; Cal. Const., art. I, § 3.) The conduct by UCSC officials jeopardizes this fundamental right.

Here, a UCSC police detective sought a search warrant for Ms. Irshad's cellphone just 15 days after she had filed a civil rights lawsuit against the UCSC Chief of Police and other UCSC officials. UCSC officers then executed the warrant mere days after Plaintiffs had filed a motion for a preliminary injunction, which relied on a declaration submitted by Ms. Irshad. The warrant included a screen shot picture of Ms. Irshad from a media interview she gave regarding this lawsuit and officers served the warrant in an extremely public manner—specifically, while Ms. Irshad stood in her pajamas in a field with hundreds of fellow students. Taken together, these events suggest that the warrant was intended to punish or intimidate Ms. Irshad for having participated in this lawsuit.

That the search warrant targeted Ms. Irshad's cellphone only deepens this sense of punishment. As discussed *supra*, her phone contains the most intimate details of her life. It also serves as a vital tool for the performance of daily tasks on campus; everything from doing laundry and homework to performing her job. Thus, to the extent it constitutes a retaliatory investigative or enforcement action following Ms. Irshad's lawful efforts to secure redress for the violation of her constitutional rights, the entire search warrant is unlawful and should be quashed. (*See Waters v. Churchill* (1994) 511 U.S. 661, 669 ["Government action based on protected speech may under

some circumstances violate the First Amendment even if the government actor honestly believes the speech is unprotected."].)

**b. Illegal Rummaging Through Protected Speech and Associations**

Because overbroad government surveillance can chill protected First Amendment activity, warrants to investigate such activity also demand heightened particularity and "the most scrupulous exactitude." (*Stanford v. State of Texas* (1965) 379 U.S. 476, 485; *accord Maryland v. Macon* (1985) 472 U.S. 463, 468.) Indeed, the problem of general "exploratory rummaging" into information about a person's beliefs, associations, and political activity poses significant threats to free speech and association and unconstitutionally chills the exercise of First Amendment freedoms. (*See Andresen v. Maryland* (1976) 427 U.S. 463, 480; *see also Marcus v. Search Warrants* (1961) 367 U.S. 717, 729 ["The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."].)

Here, Ms. Irshad has a right to freely search the internet and exchange electronic communications protected under both federal and state law. But the unfettered search of her "internet history, including cookies, bookmarks, web history, and search terms," as well as electronic communications significantly encroaches on these rights. (*See In re Malik J.*, *supra*, 240 Cal.App.4th at p. 902 [recognizing that the "unfettered" search of an electronic device and social media accounts constitutes a significant privacy invasion and modifying probation search condition accordingly]; *see, e.g.*, *Columbia Ins. Co. v. Seescandy.com* (N.D. Cal. 1999) 185 F.R.D. 573, 578 [finding limiting principles on discoverability of defendant's identity due to "legitimate and valuable right to participate in online forums anonymously"].)

This infringement is anything but trivial. As the U.S. Supreme Court acknowledged in *Packingham v. North Carolina* (2017) 582 U.S. 98, 104, the "vast democratic forums of the Internet," and "social media in particular," are among the "most important places . . . for the exchange of views." Access to the internet is necessary for "speaking and listening in the modern public square, and otherwise exploring vast realms of human thought and knowledge." (*Id.* at p. 107.) Such access is also vital to modern activism—on issues ranging from the war on Gaza to

racial justice to gun violence.[6] And it is particularly important to students like Ms. Irshad committed to carrying forward the rich history of higher learning that institutions like UCSC are supposed to foster in the critique of ideas and mainstream orthodoxies.[7]

The search warrant also directly impacts Ms. Irshad's right to free association with others. The U.S. Supreme Court has "'long understood as implicit in the right to engage in activities protected by the First Amendment a corresponding right to associate with others.'" (*Americans for Prosperity Found. v. Bonta* (2021) 594 U.S. 595, 606 [quoting *Roberts v. U.S. Jaycees* (1984) 468 U.S. 609, 622].) For instance, in *NAACP v. Alabama ex rel. Patterson* (1958) 357 U.S. 449, 462, a civil rights organization had been held in contempt for refusing to release a list of its members. The Supreme Court unanimously reversed, explaining that the "compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective [] restraint on freedom of association . . . ." (*Id.* at p. 462.) The Court recognized that "privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." (*Id.*)

Therefore, any "state action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny." (*Id.* at pp. 460–61; *see also Lyng v. Int'l Union* (1988) 485 U.S. 360, 367 fn.5 ["associational rights are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference, and . . . these rights can be abridged even by government actions that do not directly restrict individuals' ability to associate freely"] [citation and internal quotation marks omitted].)

By authorizing the unfocused search of Ms. Irshad's cellphone, including her life on the internet, geolocation data, photographs, and all electronic communications with others (among other broad expanses of information), the search warrant far exceeds what the law allows. This

---

[6] Shira Ovide, *How Social Media Has Changed Civil Rights Protests* (June 18, 2020) N.Y. Times <https://www.nytimes.com/2020/06/18/technology/social-media-protests.html> [as of Oct. 11, 2024].

[7] Richard Fausset, *From Free Speech to Free Palestine: Six Decades of Student Protest* (May 4, 2024) N.Y. Times <https://www.nytimes.com/2024/05/04/us/college-protests-free-speech.html> [as of Oct. 11, 2024].

Court should not permit UCSC police officers to rummage through the entirety of the information stored on Ms. Irshad's phone, exposing everything from the intimate details of her private life to her political and associational activities, and those with whom she associates, along with her communications with her attorneys as further discussed below.

### C. The Warrant Impermissibly Gives Defendants Access to Privileged Attorney-Client Communications and Attorney Work Product in this Litigation

The search warrant, on its face, authorizes the search of privileged attorney-client communications and protected attorney work product. It must be quashed or narrowed to ensure the confidentiality of this information. At the very least, the Court should temporarily seal Ms. Irshad's cellphone and appoint a special master to determine the applicability of these protections to the information it contains.

The attorney-client privilege is "one of the oldest recognized privileges for confidential communications." (*Swidler & Berlin v. United States* (1998) 524 U.S. 399, 403, citations omitted.) In California, the attorney-client privilege is governed by Evidence Code section 950, *et seq*., and "there are no exceptions to the privilege unless expressly provided by statute." (*Chubb & Son v. Super. Ct.* (2014) 228 Cal.App.4th 1094, 1103, citations omitted.) "[T]he client . . . has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communication between client and lawyer" if the privilege is claimed by "[t]he holder of the privilege." (Evid. Code § 954, subd. (a).) "[T]he privilege is absolute." (*Chubb & Son, supra,* 228 Cal.App.4th at 1103 [quoting *Costco Wholesale Corp. v. Super. Ct.* (2009) 47 Cal.4th 725, 732].) "Protecting the confidentiality of communications between attorney and client is fundamental to our legal system" and "a hallmark of our jurisprudence." (*People ex rel. Dept. of Corps. v. SpeeDee Oil Change Sys., Inc.* (1999) 20 Cal.4th 1135, 1146.)

The attorney work product doctrine, while separate and distinct, demands equally diligent protection. (*See* Civ. Proc. Code § 2018.030, subd. (a), (b).) '"[I]t is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel."' (*PSC Geothermal Services Co. v. Super. Ct.* (1994) 25 Cal.App.4th 1697, 1709 [quoting *Hickman v. Taylor* (1947) 329 U.S. 495, 510].). Even when disclosure of attorney work

product is involuntary, "the privilege [is] preserved if the privilege holder has made efforts 'reasonably designed' to protect and preserve the privilege." (*Regents of Univ. of Cal. v. Super. Ct.* (2008) 165 Cal. App.4th 672, 681.)

These protections apply with full force to information obtained via a search warrant. "The attorney-client and work-product privileges should not be lost simply because the prosecution seeks discovery through execution of a search warrant rather than through a discovery motion." (*PSC Geothermal Services Co.,* 25 Cal.App.4th at p. 1712.) The attorney-client privilege precludes disclosure of confidential communications via search warrant, regardless of whether formal criminal proceedings have begun. (*People v. Super. Ct.* (2001) 25 Cal.4th 703, 716.) Likewise, "materials seized pursuant to a search warrant . . . are protected by the [attorney] work product doctrine." (*Id*. at p. 718.)

Ms. Irshad's cellphone contains privileged communications. The cellphone stores text messages, phone records, voicemails, and emails sent between Ms. Irshad and her attorneys, all of which are subject to attorney-client privilege. (*See* Evid. Code, § 954.) Further, the phone contains privileged attorney work product including but not limited to draft court filings, client-interview questions, and notes on legal strategy shared with Ms. Irshad by her attorneys. (*See* Code. Civ. Proc., § 2018.030; *see also* Pen. Code, § 1054.6.) All this information is confidential and must not be disclosed to any third party, let alone to the opposing party in active litigation. The egregious overbreadth of the warrant threatens the integrity of the instant proceedings and violates well-settled legal principles codified in California law. The fact that an officer working under the supervision of a named defendant in this action willfully procured such a warrant—with constructive, if not actual knowledge of the privileged information that it would thereby jeopardize—raises ethical questions beyond the legal ones.

No exception to these protections has been demonstrated, yet the warrant permits unfettered access to all information on Ms. Irshad's phone. Even if probable cause to search certain material thought to be on Ms. Irshad's cellphone existed, probable cause alone would not automatically overcome the attorney-client and work product privileges.

Thus, if the Court is not prepared to quash the warrant outright or to narrow its scope to protect this confidential information, Ms. Irshad requests that the phone be sealed and a special master appointed pursuant to Penal Code sections 1546.1(e)(1) and (e)(2), and 1524(c), to ensure that the UCSC and UCSC Police—defendants in the civil rights litigation in which Ms. Irshad is a plaintiff—do not obtain confidential attorney-client communications or attorney work product material from the phone, and that only information necessary to achieve the objective of the warrant is accessed and any unrelated information is destroyed.

### D. The Court Should Review the Sealed Portions of the Warrant and Unseal Portions That Do Not Compromise the Investigation

Under Penal Code section 1534, a search warrant and its supporting affidavit are presumptively open to the public ten days after the warrant's issuance. (Pen. Code, § 1534, subd. (a).) The warrant here was issued over two weeks ago, and yet the affidavit and parts of the warrant remain sealed. Keeping these documents hidden from Ms. Irshad confounds the Legislature's intent to "require the notice [given to the target of a search warrant] to *include a copy of the warrant*." (Legis. Counsel's Dig., Sen. Bill No. 178 (2015-2016 Reg. Sess.) § 1 [emphasis added].) Further, it prevents Ms. Irshad from evaluating the probable cause for the warrant and from discerning the warrant's appropriate scope.

The warrant asserts good cause to seal under California Rule of Court 2.550, but it does not satisfy the high standards that Rule creates. "Unless confidentiality is required by law, court records are presumed to be open." (Cal. Rules of Court, rule 2.550(c).) Records can only be filed under seal where the court expressly finds facts establishing that sealing is the least restrictive means of achieving an overriding interest. (*Id.*, rule 2.550(d).) The sealing order must "[s]pecifically state the facts that support the findings" and seal "only those documents and pages, or, if reasonably practicable, portions of those documents and pages, that contain the material that needs to be placed under seal. All other portions of each document or page must be included in the public file." (*Id.*, rule 2.550(e).)

The order sealing the warrant here does not satisfy these rigorous requirements. It does not specifically state *any* facts, let alone facts supporting a finding that sealing the documents meets

heightened scrutiny. Though it lists "evidence destruction or tampering" as the rationale for sealing, it does not articulate the factual basis for that determination. Further, the order puts a blanket seal on the warrant, affidavit, and return, making no distinction between the "portions of those documents . . . that contain the material that needs to be place under seal" and the portions that do not. (*Ibid.*) Rule 2.550 demands greater precision. Any portions of the warrant, affidavit, and return that do not pose a risk of "evidence destruction or tampering" should be available to Ms. Irshad and to the public as part of the public file.

To that end, the Court should conduct an in camera review of the sealed portions of the warrant, affidavit, and return, and unseal the portions of these documents which do not raise a risk of evidence destruction or tampering. The Court should also redact the portions of any documents which do raise that risk and enter the redacted documents into the public record. Ms. Irshad needs access to these documents to properly evaluate the warrant's validity and its appropriate scope.

## CONCLUSION

For the foregoing reasons, the search warrant should be quashed, the phone returned to Ms. Irshad, and all information obtained pursuant to the warrant should be destroyed. Alternatively, the Court should modify the scope and cabin the time period of the search warrant, and also appoint a special master to assume custody of the phone, determine what privileged information it contains, and prevent Defendants from obtaining access to such material. Any and all records obtained pursuant to the search of Ms. Irshad's cellphone that are unrelated to the objective of the warrant should also be destroyed. (Pen. Code, §§ 1546.1, subd. (d)(2), subd. (e)(2), 1546.4 subd. (c).) Finally, Ms. Irshad requests the Court unseal the affidavit and sealed portions of the warrant that do not satisfy the heightened scrutiny required by California Rule of Court 2.550.

/

/

/

/

/

/

Dated: October 11, 2024

Respectfully submitted,

ACLU FOUNDATION OF NORTHERN CALIFORNIA, INC.
***/s/ Chessie Thacher***
Chessie Thacher (SBN 296767)
Shaila Nathu (SBN 314203)
Angelica Salceda (SBN 296152)

THE LAW OFFICE OF THOMAS C. SEABAUGH
***/s/ Thomas C. Seabaugh***
Thomas C. Seabaugh (SBN 272458)

PARTNERSHIP FOR CIVIL JUSTICE FUND, and its project, THE CENTER FOR PROTEST LAW & LITIGATION
***/s/ Rachel Lederman***
Rachel Lederman (SBN 130192)

*Attorneys for Plaintiffs*