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 Petitioner Laaila Irshad

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SANTA CRUZ

IN RE SEARCH WARRANT TO SEIZE AND SEARCH PROPERTY OF LAAILA IRSHAD

Misc. Case No.: 25CR00901
Warrant Number 24SW00396
UCSC Police Dept. Case No.: 24-582

NOTICE OF PETITION AND MOTION TO QUASH, VOID, OR MODIFY SEARCH WARRANT RE: DISCOVERY OF ELECTRONIC INFORMATION; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

(Pen. Code, § 1546.4(c))

Date: ~~To be set by the Court~~ 4/14/25
Time: ~~To be set by the Court~~ 8:15am
Dept: ~~To be set by the Court~~ D7

[Filed concurrently with Declaration of Laaila Irshad; Declaration of Thomas C. Seabaugh; and [Proposed] Order]

NOTICE OF PETITION AND

MOTION TO QUASH, VOID, OR MODIFY SEARCH WARRANT

TO DISTRICT ATTORNEY JEFFREY S. ROSELL AND TO THE CLERK OF THE ABOVE-ENTITLED COURT:

PLEASE TAKE NOTICE that, on the above listed date or as soon thereafter as the matter may be heard, Petitioner LAAILA IRSHAD will, and hereby does, petition this Court for an order voiding or modifying the search warrant for her cellphone that was issued on September 2, 2024 and executed by University of California Santa Cruz (UCSC) police officers on October 1, 2024. Ms. Irshad specifically requests that the Court quash the warrant, which she believes to have been issued under warrant number 24SW00396,[1] and order the destruction of all seized information. Ms. Irshad further petitions the Court to order the return of her seized cellphone.

Ms. Irshad seeks the relief requested pursuant to the California Electronic Communications Privacy Act (CalECPA), Penal Code section 1546 *et seq.* Subsection (c) of Section 1546.4 authorizes an individual 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 "petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of [CalECPA], or the California Constitution, or the United States Constitution." In exercising her statutory right under Section 1546.4, Ms. Irshad avers that the search warrant for her cellphone is overbroad in violation of CalECPA, the First and Fourth Amendments, and the California Constitution; and that the warrant threatens to sweep in privileged attorney-client communications and attorney work product.[2] Ms.

---

[1] Because the search warrant is sealed and because no warrant number appeared on the papers served upon Ms. Irshad, she is unable to independently verify that this search warrant number is correct. (Decl. of Laaila Irshad in Supp. of Pet. & Mot. to Quash, Two search warrants appear to be associated in the Court records database with the UCSC Police Department Case Number 24-582 that is listed on Ms. Irshad's Property and Evidence Receipt. These two warrant numbers are 24SW00298 and 24SW00396. (Decl. of Thomas Seabaugh in Supp. of Pet. & Mot. to Quash, ¶ 7.)

[2] Ms. Irshad is a plaintiff in *Ellutzi et al. v. Regents of the University of California, et al.* (Case No. 24CV02532), which is proceeding before the Hon. Syda K. Cogliati in Department 5. She

Irshad's request for the return of property is made pursuant to non-statutory rights recognized in *Gershenhorn v. Superior Court, Los Angeles County* (1964) 227 Cal.App.2d 361. (*See also Ensoniq Corp. v. Superior Court* (1998) 65 Cal.App.4th 1537.)

This Petition is based on this Notice of Petition and Motion; the Memorandum of Points and Authorities herein; and the supporting Declarations of Laaila Irshad and Thomas C. Seabaugh filed concurrently herewith; as well as any further argument or authorities that may be requested or permitted by the Court.

Dated: March 5, 2025

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 Petitioner

previously sought to quash the search warrant via a motion filed in that civil case. On February 10, 2025, however, Judge Cogliati denied the motion without prejudice on the ground that it could not be resolved in that case, ordering instead that Ms. Irshad could "file[] under CalECPA with the Criminal Division of the Santa Cruz Superior Court." (Seabaugh Decl., ¶ 4; Ex. C.)

MEMORANDUM OF POINTS AND AUTHORITIES

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes **Page(s)**

Rules **Page(s)**

I. INTRODUCTION

Laaila Irshad respectfully petitions the Court for an order quashing the search warrant for her cellphone that was issued on September 25, 2024 and executed by UCSC police officers six days later. Ms. Irshad brings this petition 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 "petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of [CalECPA], or the California Constitution, or the United States Constitution." The warrant here is largely unbounded as to time and scope, and lacks the particularity required by law. The search that it authorizes sweeps in an enormous range of Ms. Irshad's private and sensitive communications, location, photographic, and internet search history data dating back to before Ms. Irshad was even a UCSC student. It also sweeps in attorney-client privileged communications and attorney work product related to the civil rights action that Ms. Irshad filed against UCSC in connection with protests on campus last spring. The warrant especially smacks of retaliation given that a UCSC officer sought the warrant just two weeks after Ms. Irshad had initiated the civil rights action against the school, and officers then executed it in a manner designed to be maximally public and embarrassing—that is, while Ms. Irshad stood in her pajamas in a field with hundreds of other students after an early morning fire drill. Because the warrant violates CalECPA, the First and Fourth Amendments, and the California Constitution, it should be quashed and voided or, at a minimum, modified.

II. STATEMENT OF FACTS

A. Laaila Irshad's Role as Plaintiff in Ongoing Civil Rights Litigation

Ms. Irshad is a third-year undergraduate student and Resident Advisor at UCSC. (Irshad Decl., ¶ 2.) On September 9, 2024, Ms. Irshad commenced a civil rights action in Santa Cruz Superior Court with two other plaintiffs alleging that UCSC had violated their due process rights by banishing them and more than 100 other students from campus during a protest in May 2024. (*See Ellutzi, et al. v. Regents of the University of California, et al.,* Case No. 24CV02532.) The

lawsuit named, among other defendants, Kevin Domby, in his official capacity as UCSC Chief of Police and Executive Director of Public Safety. (Seabaugh Decl., ¶ 2; Ex. A.) Ms. Irshad and the other plaintiffs filed a motion for a preliminary injunction on September 26, 2024. (*Id.*, ¶ 3.) Just five days later, a member of the UCSC police executed a sealed warrant authorizing the seizure and search of Ms. Irshad's cellphone for evidence of alleged vandalism. (Irshad Decl., Ex. A.)

B. Heavy-Handed 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.) Still in her pajamas, Ms. Irshad knocked on doors to alert students of the alarm and helped guide 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 standing there, UCSC police officers approached, took her cellphone, and served her with a search warrant. (*Id.*, ¶¶ 4-5.) It was a very public and embarrassing encounter that left Ms. Irshad with the impression that she was being singled out for punishment. (*Id.*, ¶ 5.)

The warrant included a "screenshot" picture of Ms. Irshad being interviewed by KSBW Action News 8 about the filing of her civil rights case. (*Id.*, ¶ 6.) Accompanying that news segment was an article entitled "UC Santa Cruz Faces Lawsuit Over Handling of Campus Protests." (*Ibid.*) UCSC officers used this screenshot of Ms. Irshad even though the school had access to her student ID photo—which further reinforced the belief that she was being punished for participating in litigation against UCSC. (*Ibid.*) The cellphone that UCSC officers ultimately seized had photos, data, and other personal information dating back to when Ms. Irshad was in Fifth Grade. (Irshad Decl. ¶ 7.)[3]

Ms. Irshad experienced significant hardships because of the seizure of her cellphone. (*Id.*, ¶¶ 7-10.) Her phone held a wide range of personal information, including her contacts and telephone numbers, internet search caches, pictures of friends and family, banking accounts, medical information, and many intensely emotional and sensitive emails and text messages. (*Id.*, ¶

[3] The cellphone held data dating back to this earlier period in Ms. Irshad's life because, as is a common practice, Ms. Irshad activated her new cellphone by importing all of the data that had been stored on her last cellphone or in her cloud-based account. (Irshad Decl., ¶ 11.)

7.) Her phone also contained emails, voicemails, and text messages exchanged with undersigned counsel about her civil rights action. (*Id.*, ¶ 8.) Without her phone, Ms. Irshad 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 also struggled to access her UCSC email and student portal, and to complete class assignments on the portal. (*Id.* ¶ 9.) Apps on her phone were also essential for her work responsibilities and accessing campus services. (*Id.* ¶ 10.) It was even difficult for Ms. Irshad to do her laundry because the campus machines operate by scanning QR codes for payment. (*Ibid.*) Ms. Irshad did not have funds sufficient to purchase a phone on her own and was only able to secure a replacement after friends and community members raised money for the purchase. (*Id.*, ¶ 11.) Both the disruption and financial burden of the phone seizure were significant.

C. Overbroad Scope of Search Authorized by Warrant

The Search Warrant, issued on September 25, 2024, authorized 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 otherwise sealed search warrant and is unable to review the sealed affidavit in support, this Petition focuses on the warrant's overbreadth and deficiencies of particularity. It proceeds in five parts: ***First***, the Petition sets forth the governing CalECPA framework; ***Second***, the Petition explains why the search warrant's overbreadth violates CalECPA, as well as both federal and state constitutional law; ***Third***, the Petition establishes that the search warrant risks compromising attorney work product and attorney-client privileged communications; ***Fourth***, the Petition argues that the Court should evaluate the basis for the continued sealing of portions of the warrant and affidavit; and ***Fifth***, the Petition explains that Ms. Irshad's cellphone should be returned to her, as its continued official retention violates her constitutional rights.

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, 396 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 California 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.[4]

---

[4] 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/>).

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 . . . ." (*Id.*, § 1546.1, subd. (d)(l), emphasis added.)

CalECPA's heightened particularity requirement is a direct response to the conclusion in *Riley* that government officials should not be allowed to broadly rummage through 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 "include, for example, medical records, financial records, personal diaries, and intimate correspondence with family and friends." (*Ibid.*)

2. Explicit Remedies for any Violation

One prominent feature of CalECPA's 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 violates 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); *see also Saunders v. Superior Court* (2017) 12 Cal.App.5th Supp. 1, 22–23 [CalECPA "provides additional privacy protections" and remedies given the "heightened privacy concerns in both cellphone records and content"]; *Elkins v. United States* (1960) 364 U.S. 206, 217 [emphasizing importance of robust remedies].)[5]

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.

B. The 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

When measured against the rubric of the Fourth Amendment and CalECPA, the search warrant for Ms. Irshad's cellphone fails the test. Both require that a warrant describe with particularity not only the material that can be ***seized***, but also the specific areas, things, and "time periods" that can be ***searched*** for that material. (Pen. Code, § 1546.1, subd. (d)(1).) This particularity requirement prevents overbroad searches and serves as a buttress against "reviled 'general warrants'" with the government's "rummaging" through our personal lives. (*Riley, supra*, 573 U.S. at p. 403.) The particularity requirement's corollary is that any warrant authorizing a privacy invasion be "as limited as possible." (*Coolidge v. New Hampshire* (1971) 403 U.S. 443, 467.) Indeed, "[b]y limiting the authorization to search to the specific areas and things for which

---

[5] That CalECPA authorizes the voiding of a warrant or 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. (*See* Cal. Const., art. I, § 28, subd.(f)(1).) The two-thirds majority was necessary 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.)

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." (*DiMaggio v. Superior Court* (2024) 104 Cal.App.5th 875, 887.)

To determine if 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.'" (*United States 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) 90 Cal.App.5th 520, 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 pp. 529–40; *see Kow, supra,* 58 F.3d 423 at p. 427 [warrant not sufficiently particular where it did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place]; *see also United States v. McCall* (11th Cir. 2023) 84 F.4th 1317, 1328 ["By narrowing a search to the data created or uploaded during a relevant time connected to the crime being investigated, officers can particularize their searches to avoid general rummaging."].)

Nowhere are these constitutional principles more apt than when the search target is one's digital device, which contains electronic information that is susceptible to "over-seizing." As the Ninth Circuit explained in *United States v. Schesso* (9th Cir. 2013) 730 F.3d 1040: "Because electronic devices c[an] contain vast quantities of intermingled information, raising the risks inherent in over-seizing data, law enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence." (*Id.* at p. 1042; *Appleton*, *supra*, 245 Cal.App.4th at pp. 725-26 [as soon as an officer views personal information during the execution of a search, privacy interests are "compromised"].)

The search warrant at issue here flies in the face of this law. It permits the search of virtually *all* data stored on Ms. Irshad's 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." (*Ibid.*) It is hard to reconcile how a search with

such an unfixed beginning date could be tethered to a time-bounded act of alleged vandalism—an offense not characterized by yearslong planning, premeditation, or internet searches.

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 "the date of inception of first data storage" and by failing to address how data imported from any of Ms. Irshad's prior digital devices should be treated, the warrant improperly authorizes the search of Ms. Irshad's entire digital life. Moreover, because Ms. Irshad stored data on her device dating back to when she was in Fifth Grade (Irshad Decl. ¶¶ 7, 11), the search of her cellphone is certain to sweep in data that predates not just any incident UCSC police might be investigating, but even her time as a UCSC student. There is simply no legitimate reason for UCSC officers to rummage through everything on Ms. Irshad's phone from first use to present.

The warrant's scope is similarly unrestricted. It authorizes a search of everything from Ms. Irshad's internet search history to her texts with family to the metadata on every one of her photographs. And the warrant vaguely identifies items of information to be seized as the "evidence and instrumentalities" of vandalism. But as is relevant here, some courts have found warrants overbroad even when the warrant confined a "search to only records that are evidence of the violation of a certain statute." (*United States v. Cardwell* (9th Cir. 1982) 680 F.2d 75, 77-78; *see also United States v. Clark* (9th Cir. 1994) 31 F.3d 831, 836 [holding that warrant authorizing search for "narcotic controlled substances, drug paraphernalia, marijuana cultivation equipment, instructions, notes, cultivation magazines, currency, documents, and records and fruits and instrumentalities of [a] violation of Title 21 U.S.C. § 841(a)(1)" was "facially overbroad" because it provided "no guidance" about the "fruit or instrumentality of the alleged crime"].)

The warrant in this case covers a nebulous, nearly unrestricted time period and fails to describe with particularity the items to be seized, making it indistinguishable from an unconstitutional general warrant. Under CalECPA and the Fourth Amendment, these failures justify the Court's swift intervention.

2. The Warrant is Overbroad in Violation of Ms. Irshad's Rights to Free Speech, Free Expression, and Free Association

The First Amendment and the California Constitution protect Ms. Irshad's act of filing her lawsuit against UCSC, as well as her expressions of dissent and free association. And yet, the warrant impermissibly encroached on these rights by authorizing law enforcement to examine years' worth of internet searches, geolocation data, photographs, and electronic information—without any meaningful temporal limits relating to the vandalism alleged. The warrant also invaded the constitutional and privacy rights of the persons with whom Ms. Irshad associated.

a. Retaliatory Search and Seizure

The First Amendment protects "vigorous advocacy" and the right to access the courts free from retaliation, including retaliatory investigative or enforcement actions. (*NAACP v. Button* (1963) 371 U.S. 415, 429-30; *see also Powell v. Alexander* (1st Cir. 2004) 391 F.3d 1, 20 [recognizing that the First Amendment protects the filing of a civil rights lawsuit and that any retaliation for filing such a lawsuit "risked violating" that constitutional right]; *see also Bridges v. Gilbert* (7th Cir. 2009) 557 F.3d 541, 551 [First Amendment also guarantees right to be free from retaliation for providing affidavit against officers]; *Waters v. Churchill* (1994) 511 U.S. 661, 669.)

Here, the chronology of events gives rise to the impression that UCSC police officers punished Ms. Irshad for having exercised her right to seek redress for alleged constitutional violations. A UCSC officer sought the warrant just 15 days after Ms. Irshad filed her civil rights lawsuit against UCSC and the Chief of Police. Officers then executed the warrant in a maximally public and embarrassing manner mere days after she filed a preliminary injunction motion. The warrant directly implicated the civil rights lawsuit by including the screenshot of Ms. Irshad giving an interview about the case. And the action had a particularly punitive and chilling impact because Ms. Irshad's cellphone was essential to the performance of her daily tasks and contained deeply private information, including attorney-client communications.

b. Invasive Rummaging Through Protected Speech and Associations

The unfettered search of Ms. Irshad's internet history, social media, and electronic communications also significantly encroached on her constitutional rights of privacy, free speech,

and political advocacy—as well as the rights of those with whom she communicated on her device. (*See, e.g.*, *In re Malik J.* (2015) 240 Cal.App.4th 896, 902 [recognizing "threat of unfettered searches" to both the individual targeted and "third parties' constitutional rights of privacy and free speech]; *accord Gibson v. Fla. Legis. Investigation Com.* (1963) 372 U.S. 539, 546; *Meza*, *supra*, 90 Cal.App.5th at p. 540.)

Ms. Irshad has a First Amendment right to receive information and ideas over the internet as well as to express them. (*See Kleindienst v. Mandel* (1972) 408 U.S. 753, 762.) The United States Supreme Court has deemed the internet—and particularly social media—to be the most important place for the exchange of views today. (*Packingham v. North Carolina* (2017) 582 U.S. 98, 104.) California courts are in accord: "The architecture of the Internet, as it is right now, is perhaps the most important model of free speech since the founding [of the Republic]." (*In re Stevens* (2004) 119 Cal.App.4th 1228, 1236.)

The First Amendment also protects Ms. Irshad's records of political association and expression on her phone. The government's "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. (*Andresen v. Maryland* (1976) 427 U.S. 463, 479.) As the Supreme Court explained in *Lyng v. International Union* (1988) 485 U.S. 360: "[A]ssociational 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." (*Id.* at p. 367 n.5 [citation and internal quotation marks omitted].)

In this context, the First Amendment protects from disclosure the opinions on political subjects that Ms. Irshad has expressed to others, the conversations that she may have participated in anonymously, and the identities of those with whom she lawfully associated for political purposes. "[P]rivacy in group association" is "indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs," and "compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective [] restraint on freedom of association." (*NAACP v. Alabama ex rel. Patterson* (1958) 357 U.S. 449, 462; *Columbia Ins.*

Co. v. Seescandy.com (N.D. Cal. 1999) 185 F.R.D. 573, 578 [limiting principles on discoverability of identity due to "legitimate and valuable right to participate in online forums anonymously"].)

Accordingly, although the Fourth Amendment standards themselves do not change when expressive or associational material is at issue, courts have recognized for more than fifty years that the Fourth Amendment standard must be applied with "the most scrupulous exactitude" when material about First Amendment activity is at issue. (*Stanford v. Texas* (1965) 379 U.S. 476, 485; *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."]; *Meza*, *supra*, 90 Cal.App.5th at p. 540 ["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"] [citation omitted].).

The search warrant for Ms. Irshad's cellphone fails this "scrupulous exactitude" test. It allows UCSC officers to rummage through all of the information stored on her device, exposing everything from the intimate details of her private life to her political and associational activities, along with her communications with third parties and her attorneys. The known presence on Ms. Irshad's cellphone of such sensitive information and First Amendment-protected activity should have provided UCSC officers with even more impetus for a carefully drawn and circumscribed search. But they pursued the opposite tack, executing an overbroad and punitive warrant that was far more invasive than what could conceivably be necessary to investigate alleged vandalism.

C. The Warrant Impermissibly Gives UCSC and UCSC Officers Access to Privileged Attorney-Client Communications and Attorney Work Product

The search warrant provides UCSC police officers access to—and permits the search of—privileged communications and protected attorney work product related to Ms. Irshad's civil rights case naming the UCSC Chief of Police as a defendant. This impropriety provides reason to quash or modify the warrant and raises ethical questions as to whether UCSC officers informed the court about the pending civil rights case when they sought authorization for the expansive search of Ms. Irshad's device.

Here, while the search warrant does not permit UCSC officers to seize the privileged communications and attorney work product on Ms. Irshad's device, it does allow them to search this information. And it is this disclosure to parties who are adverse to Ms. Irshad in a legal action that presents a cognizable harm. (*See People v. Superior Court* (*Laff*) (2001) 25 Cal.4th 703, 716-19 [recognizing that materials seized pursuant to a search warrant do not lose protection of attorney-client privilege or work-product doctrine]; *see also Mitchell v. Superior Court* (1984) 37 Cal.3d 591, 599 ["[T]he fundamental purpose behind the [attorney-client] privilege is to safeguard the confidential relationship between clients and their attorneys . . . ."].)[6]

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.) In California, the attorney-client privilege is governed by statute (Evid. Code, §§ 950, 954), and "there are no exceptions to the privilege unless expressly provided by statute." (*Chubb & Son v. Super. Court* (2014) 228 Cal.App.4th 1094, 1103). "Protecting the confidentiality of communications between attorney and client is fundamental to our legal system" and "a hallmark of our jurisprudence." (*People ex rel. Dep't 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.) "[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. Superior Court* (1994) 25 Cal.App.4th 1697, 1709 [quotations omitted].). Even when disclosure of 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 California v. Superior Court* (2008) 165 Cal.App.4th 672, 681.)

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

---

[6] In the civil rights case proceeding in Department 5, the parties agreed on the record that defense counsel would not receive or use any non-public information obtained from Ms. Irshad's cellphone pursuant to the warrant. (Seabaugh Decl., ¶ 3; Ex. B at 53:19-54:22.)

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; Pen. Code, § 1054.6.) This information is all confidential and must not be accessible to any third party, let alone to UCSC officers who might serve as adverse percipient witnesses in Ms. Irshad's civil rights action and be asked to testify or provide facts about Ms. Irshad, the other plaintiffs, or the campus-wide protests during the 2023-2024 academic year.

The egregious overbreadth of the warrant threatens the integrity of the proceedings in Ms. Irshad's civil matter and violates well-settled legal principles codified in California law. Once privileged materials have been reviewed, there is no way to erase the knowledge gained. The risk of an unfair advantage or misuse—even inadvertent—is high. (*See Laff, supra*, 25 Cal.4th at p. 719.) Thus, to ensure the privileged or confidential nature of information on Ms. Irshad's device, the search warrant must be quashed or narrowed. Alternatively, if this Court is not prepared to quash the warrant outright or to narrow its scope, the Court should seal Ms. Irshad's cellphone and hold an *in camera* hearing to review the cellphone data collected and screen out any privileged or protected material. (*See* Pen. Code, § 1546.1, subd. (e); *see also People v. Superior Court (Bauman & Rose)* (1995) 37 Cal.App.4th 1757, 1768-69 ["The probable cause showing for the warrant does not obviate the need for an in camera hearing on whether the privilege[s] appl[y] to seized materials."]; *Laff, supra*, 25 Cal.4th at p. 720.)

D. The Court Should Evaluate the Basis for Sealing the Warrant

Under California law, 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); Cal. Rules of Court, rule 2.550(c).) The warrant here was issued months ago, and yet the affidavit and parts of the warrant remain sealed. Keeping these documents hidden from Ms. Irshad deprives her of an opportunity to defend herself and 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].).

The warrant asserts good cause to seal under California Rule of Court 2.550, but it does not satisfy the high standards that this Rule creates. Pursuant to Rule 2.550, records can be filed

under seal only where the court expressly finds facts establishing that sealing is the least restrictive means of achieving an overriding interest. (Cal. Rules of Court, 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." (Cal. Rules of Court, rule 2.550(e).) The order sealing the warrant does not appear to satisfy these rigorous requirements.

E. The Court Should Order the Return of Ms. Irshad's Cellphone

Pursuant to *Gershenhorn v. Superior Court, Los Angeles County* (1964) 227 Cal.App.2d 361, Ms. Irshad requests that the Court order the return of her cellphone. The right to regain possession of one's property is a "substantial right." (*Franklin v. Municipal Court* (1972) 26 Cal.App.3d 884, 896.) And both criminal defendants and nondefendants alike may move for the return of seized property on the basis that a search warrant or seizure was unlawful. (*Ensoniq,* 65 Cal.App.4th at p. 1537.) Here, Ms. Irshad's cellphone was taken on October 1, 2024—more than five months ago. The continued retention of her property with no criminal action pending violates Ms. Irshad's due process rights—especially, when UCSC officers have had the capacity and opportunity to seize all data subject to the search warrant and should no longer require possession of the physical device. (*People v. Lamonte* (1997) 53 Cal.App.4th 544, 549.)

IV. CONCLUSION

The warrant should be quashed, the phone returned to Ms. Irshad, and all information obtained pursuant to the warrant destroyed. (Pen. Code, §§ 1546.1(d)(2), (e)(2), 1546.4(c) (authorizing courts to "order the destruction of any information obtained in violation of this chapter").

/

/

/

/

/

Dated: March 5, 2025

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 Petitioner