Case No. ____

IN THE SUPREME COURT FOR THE STATE OF CALIFORNIA

MICROSOFT CORP.
Petitioner,

v.

SUPERIOR COURT OF LOS ANGELES COUNTY,
Respondent,

CITY OF LOS ANGELES,
Real Party in Interest.

After a Decision by the Court of Appeal
Second Appellate District, Division Four, Case No. B347381

On A Petition for a Writ of Mandate From the Superior Court of Los Angeles County,
Case No. 25CJGO00165, Hon. Craig Richman, Presiding

PETITION FOR REVIEW

*James R. Sigel (SBN 288478)
DAVIS WRIGHT TREMAINE LLP
50 California Street, Suite 2300
San Francisco, CA 94111
Telephone: (415) 276-4850
Email: jamessigel@dwt.com

Alexander F. Porter (SBN 258597)
DAVIS WRIGHT TREMAINE LLP
350 South Grand Avenue, 27th Fl.
Los Angeles, CA 90071
Telephone: (213) 633-6800
Email: alexporter@dwt.com

Ambika Kumar (*pro hac vice forthcoming*)
MaryAnn T. Almeida (*pro hac vice forthcoming*)
Shontee M. Pant (SBN 344797)
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue, Suite 3300
Seattle, WA 98104-1610
Telephone: (206) 757-8030
Email: ambikakumar@dwt.com
Email: maryannalmeida@dwt.com
Email: shonteepant@dwt.com

Attorneys for Petitioner Microsoft Corporation

PUBLIC - Redacts Materials From Conditionally Sealed Record

CERTIFICATE OF INTERESTED PARTIES

In accordance with Rule 8.208 of the California Rules of Court, the undersigned certifies that other than the Parties, [redacted] may have a financial or other interest in the outcome of this proceeding that the justices should consider in determining whether to disqualify themselves.

Dated: July 28, 2025

/s/ James R. Sigel
James R. Sigel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Constitutional Provisions

OTHER AUTHORITIES

ISSUES PRESENTED FOR REVIEW

1. Does the California Electronic Communications Privacy Act ("CalECPA") require the government to provide a factual basis "to believe that notification may have an adverse result" (Pen. Code, § 1546.2, subd. (b)(1)) before a court imposes a secrecy order, or may the court rely on the supposition that law enforcement has a reason for requesting secrecy?

2. Do the First Amendment to the U.S. Constitution and Article I, Section 1 of the California Constitution require the government to justify a CalECPA secrecy order's content-based prior restraint on speech by presenting evidence showing that no less restrictive alternative will achieve its compelling interest?

INTRODUCTION

This petition for review raises questions for which this Court's guidance is critically needed: what must the government show to justify a broad restriction on a cloud services provider's speech under the California Electronic Communications Privacy Act? Over a thousand CalECPA secrecy orders are issued every year, and many of them implicate difficult and important free speech issues. But as of yet, *no* California precedent addresses the permissible scope of these secrecy orders. Given the relatively short duration of such orders, and the difficulties that parties who are subject to them face in securing appellate review, these important questions will continue to evade scrutiny unless this Court steps in.

This case presents an ideal vehicle to address these important issues. In May 2025, Microsoft received a secrecy order accompanying a CalECPA warrant, which barred Microsoft from telling its customer, [redacted], that the Los Angeles Police Department (LAPD) seized data belonging to [redacted] and stored by Microsoft in the cloud. The LAPD sought data for just one of [redacted]'s approximately [redacted] email accounts, this one assigned to [redacted]. But the LAPD secured an order that prohibits Microsoft from notifying a trusted contact at [redacted] of the existence of the warrant—or even of the fact that Microsoft complied with legal process involving a single, unnamed account.

The Superior Court upheld this blanket prohibition on Microsoft's speech. It did so even though [redacted] is not the target of the LAPD's investigation, and even though the City of Los Angeles (City) and the court all but admitted there is no basis in the record to believe that informing a trustworthy contact at [redacted] of the warrant's existence (or of the mere fact of legal process) would impede the investigation. Instead, the trial court ultimately relied on its own speculation that the LAPD detective who sought the warrant might have undisclosed reasons for prohibiting anyone at [redacted] from being informed of its existence. The Court of Appeal then summarily denied Microsoft's petition for a writ of mandate.

Microsoft now asks this Court to provide much-needed guidance to the lower courts on the showing necessary when restricting a cloud services provider's speech under CalECPA. It should make clear that in evaluating such secrecy orders, courts must hold the government to its burden to show that the full scope of its suppression of speech is justified—consistent with the First Amendment to the U.S. Constitution, Article I, Section 1 of the California Constitution, and CalECPA itself.

These issues are important to the public because Californians deserve transparency into law enforcement demands for their data stored in the cloud. These issues are also significant for cloud services providers, as they store data for businesses in California and have an interest in ensuring CalECPA is not abused. And while the particular secrecy order in question is, absent an extension, set to expire on July 31, 2025, these open questions about unsupported secrecy orders will recur frequently, given the thousands of CalECPA warrants issued across the state each year.

The D.C. Circuit recently made clear that under the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2713, the federal analogue to CalECPA, the government's mere *assertion* of a need for secrecy is not enough to justify a secrecy order. Rather, the government must present actual, specific evidence demonstrating the need for secrecy. (*In Re Sealed Case* (D.C. Cir. July 18, 2025, No. 24-5089) 2025 WL 2013687.) This Court should use this opportunity to clarify that the same is true in California under CalECPA—which is intended to be even more protective of private parties' rights.

Microsoft's petition for review should be granted.

BACKGROUND

A. Requests for Data Held by Cloud Service Providers

For centuries, businesses stored records in paper files, and law enforcement had to serve legal process on the company directly to get those records. This process was transparent. The business knew what the government was doing and what it seized. As a result, it could object, assert privilege, or otherwise protect its legal interests.

The advent of computers did not materially change the available investigative tools. Twenty years ago, a company typically stored its information on a server on the company's physical property. Just as the government would obtain a search warrant for physical evidence, "prosecutors had to approach a company or similar enterprise directly for electronic data" stored on its servers. (U.S. Dep't of Justice, *Seeking Enterprise Customer Data Held by Cloud Service Providers* (Dec. 2017) ("DOJ Recommended Practices"); Vol. I, Ex. 2, p. 45.)

Cloud computing, however, changed this dynamic. Companies and other organizations generally now store information in the "cloud"—i.e., on remote servers owned by cloud services providers like Microsoft. The government has sometimes capitalized on this change by requiring cloud providers to produce customers' data rather than going to the customers directly. It often obtains secrecy orders when it does so, enabling it to seize data and records without the company's knowledge, unlike with a traditional warrant.

This new power allows the government to gather evidence in secret. But it comes with a cost to transparency and to the data's owners: without knowing about the seizure of their data and records, companies cannot act to protect their rights.

B. CalECPA Establishes Important Privacy Protections

In 2015, California enacted CalECPA to create a "clear, uniform warrant rule for California law enforcement access to electronic information." (SB No.178 Privacy: electronic communications: search warrant, Assembly Floor Analysis (Sept. 4, 2015)[1]; Vol. I, Ex. 2, p. 54.) The statute was passed to establish guardrails limiting the government's access to electronic data and to improve on its nearly 40-year-old federal analog, the SCA. (*Ibid.*) After its enactment, CalECPA was celebrated for "how it significantly improves on federal law," and described as "the most privacy-protective legislation of its kind in the nation." (Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)* (2018) 33 Berkeley Tech. L.J. 131, 133.)

Under CalECPA, the government must obtain a warrant to obtain the content of electronic communications. (Pen. Code, §§ 1546.1, 1546.2, subd. (a)(1).) CalECPA generally requires notice to a customer or subscriber "contemporaneously with the execution of a warrant." (*Id.* § 1546.2, subd. (a)(1).) But it permits courts to forbid disclosure to the customer where there is "reason

[1] https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160SB178 (last visited July 25, 2025).

to believe” notice may result in a specified adverse result: “Danger to the life or physical safety of an individual”; “Flight from prosecution”; “Destruction of or tampering with evidence”; “Intimidation of potential witnesses”; or “Serious jeopardy to an investigation or undue delay of a trial.” (*Id.* § 1546, subd. (a).) Such orders prohibiting disclosure to the subscriber or customer may last only for 90 days at a time. (*Id.* § 1546.2, subd. (b)(1).)

CalECPA warrants are frequently used to obtain data in California. Microsoft alone received over three hundred such warrants in each of the last three years, with the number increasing each year. (Petition for a Writ of Mandate From the Superior Court of Los Angeles County, Case No. 25CJGO00165 (“Pet.”) p. 15.)

C. Microsoft’s Cloud Services and Privacy Commitments

Microsoft provides online services, including Microsoft 365, to individual and enterprise customers. Microsoft 365 operates in the cloud. When an enterprise customer signs up for Microsoft 365, it purchases a specified number of end-user licenses, or “seats,” each of which the customer may assign to an individual user who receives account credentials and an email address. (Vol. I, Ex. 3, p. 173, ¶ 4.)

Microsoft has industry-leading privacy policies and practices, and it devotes substantial resources to protecting its customers’ data and complying with privacy laws. A core principle of Microsoft’s privacy commitments for Microsoft 365, set forth in its contracts, is that the customer’s data belongs to the customer, not to Microsoft. (Vol. I, Ex. 3, pp. 175 ¶ 8, 176 ¶ 10, 177 ¶12.)

Thus, when law enforcement seeks enterprise data from Microsoft, Microsoft tries to redirect law enforcement to the customer. And before complying with a request, Microsoft generally notifies the customer—unless it receives a secrecy order forbidding it from doing so. These practices allow customers to keep the same level of control over their data as when they store that data on their own servers. (Vol. I, Ex. 3, pp. 175-176 ¶ 8, 176 ¶ 10, 177 ¶ 12.)

Consistent with these commitments, Microsoft regularly works with law enforcement to identify ways to notify its customers of law enforcement demands, even where the government initially obtains a gag order. Notification of an enterprise when law enforcement seeks data from a limited number of accounts is consistent with U.S. Department of Justice guidance and policy on warrants under the less protective SCA. Under DOJ recommendations, law enforcement should "seek data directly from the enterprise" and not its cloud provider, except where that enterprise is "essentially devoted to criminal activity—for example, a small medical practice suspected of engaging in massive Medicare fraud." (DOJ Recommended Practices; Vol. I, Ex. 2, p. 46.)

D. The Warrant

On May 2, 2025, Microsoft received a search warrant for content data associated with a single individual account with an [redacted] email address, in connection with [redacted] investigation.

(Vol. I, Ex. 2, pp. 38-43; Pet. p.17.) [redacted] has assigned more than [redacted] end-user licenses to individual users, each of whom has account credentials and an email address. (Vol. I, Ex. 3, p. 175-176 ¶ 11.) The individual user to whom this account is assigned appears to be [redacted]. (Vol. I, Ex. 2, pp. 38-43, 86-99.) Microsoft produced the data sought by the warrant on May 12, 2025. (Vol. I, Ex. 3, p. 177 ¶ 13.)

The search warrant came with a secrecy order, which bars Microsoft from disclosing the search warrant for [redacted]” (Vol. I, Ex. 2, pp. 38-43.) The secrecy order is set to expire on July 31, 2025. (See *ibid.*)[2] The City has not stated whether it intends to apply for an extension of the secrecy order.

E. Microsoft Seeks To Notify Its Customer

LAPD Detective [redacted] submitted an affidavit—which was filed and remains ex parte—in support of the application for the warrant. When Microsoft received the warrant and secrecy order, it promptly contacted Detective [redacted] to request that Microsoft be permitted to provide notice to [redacted]—not the target—about the warrant. (Pet. at p. 18.)

[2] Although Microsoft believes the order should actually expire July 30, the City maintained before the trial court that CalECPA is ambiguous as to when the 90-day clock starts, and the trial court assumed “in the interest of caution” that July 31 would be the 90th day. (Vol. II, Ex. 15, p. 361:4-7.)

On May 13, 2025, Detective [redacted] responded by email, saying that he had "spoke[n] directly with the judge about your request. His order still stands. Both the LAPD and Microsoft are ordered not to disclose the existence of the warrant to [redacted]." (*Ibid.*) Detective [redacted] also stated that Microsoft's proposal "is not up for discussion." (*Ibid.*)

Over the next two weeks, Microsoft sought to engage the City about the possibility of notifying [redacted] of the existence of the warrant. Microsoft proposed notification to a single individual at [redacted], identifying candidates, [redacted]. Microsoft also proposed notifying [redacted] only of the existence of a warrant from the LAPD, not its target. The City rejected Microsoft's proposals. (Vol. I, Ex. 2, p. 33 ¶ 3, p. 34 ¶ 9.) In doing so, the City Attorney refused to provide any information regarding the justification for the secrecy order.

F. Microsoft's Motion To Modify The Secrecy Order

On May 28, 2025, Microsoft filed a motion to modify the secrecy order. Microsoft did not seek to set aside the secrecy order entirely, or ask to notify the target of the investigation about the warrant. Instead, Microsoft again identified multiple potential candidates at [redacted] whom Microsoft believed it could safely notify about the warrant based on publicly available information about these candidates. [redacted]'s institutional structure and regulatory and compliance mechanisms suggest many other people could safely be notified of the existence of the warrant if these candidates were deemed inappropriate.

As Microsoft emphasized, [redacted]'s interests in keeping [redacted] safe would also align with law enforcement's goals in an investigation. There is no indication that [redacted] is implicated in any wrongdoing, and the nature of the [redacted] suggests that it is not.

G. The City's Opposition

The City opposed Microsoft's motion to modify. Although it asserted that Microsoft's proposed disclosures would threaten the ongoing investigation, it did not provide any evidence or even rationale to support that contention. Instead, the City maintained it was not required to show that disclosure to Microsoft's identified candidates would pose a risk.

H. The June 18, 2025, Hearing And Attempted Resolution

At the hearing on Microsoft's motion, the trial court proposed, and Microsoft agreed, to the compromise Microsoft had offered in the beginning—i.e., to provide a contact at [redacted] with notice of the fact of a warrant from the LAPD but no further details, such as the identity of the target. The trial court stated it would be comfortable with this proposed notice, which was "not moving very far off of ground zero" on nondisclosure. (Vol. II, Ex. 14, p. 321:16-19.) The City said it would agree to that disclosure, pending confirmation from Detective [redacted]. (Vol. II, Ex. 14, p. 323:26-27.) The City professed that the proposed notice was so minimal that it did not "even know why we are having this discussion." (Vol. II, Ex. 14, p. 322:9-10.)

I. Microsoft's Proposed Order

Consistent with this tentative agreement, Microsoft prepared a draft proposed order, which it provided to the City Attorney on June 19, 2025. The proposed order would have permitted Microsoft to notify a contact at [redacted] that Microsoft had received a warrant from the LAPD for data from a single email account belonging to [redacted], and that Microsoft had sought and obtained a modification of the accompanying secrecy order to permit it to notify a contact at [redacted] of the warrant's existence and of Microsoft's production of responsive data. The proposed notice would also have provided the [redacted] contact with Detective [redacted]' contact information (or another contact as determined by the City) for any further questions. (Vol. II, Ex. 16, pp. 365-367.)

On June 21, 2025, however, counsel for the City informed Microsoft that she had "talk[ed] to Detective [redacted]" and "[t]he proposal is not acceptable." (Pet. p. 22.)

J. The June 24, 2025, Hearing And Ruling

Because the City did not agree to the court-brokered compromise, the parties appeared for a second hearing on June 24, 2025. At that hearing, the City asserted: "The Detective's position is, no." (Vol. II, Ex. 15, p. 342:14.) The City provided no explanation for that position, and it admitted the detective himself "did not offer any more" explanation. (Vol. II, Ex. 15, p. 342:21-22.)

The trial court denied Microsoft's motion to modify the secrecy order because Detective [redacted] had refused the compromise. The court made no findings that the statutory factors that might preclude disclosure were satisfied with respect to [redacted]. Nor did it explain how the secrecy order was narrowly tailored given the alternatives Microsoft had proposed, instead declining to consider Microsoft's candidates for notification. (Vol. II, Ex. 15, p. 351:5-8.)

Notably, the trial court indicated that the ex parte affidavit Detective [redacted] originally submitted would not itself justify the breadth of the order. Instead, the court speculated that Detective [redacted] may have "more information potentially than was contained in the search warrant affidavit" underlying the secrecy order. (Vol. II, Ex. 15, p. 356:21-25.)[3]

K. Microsoft's Petition For A Writ Of Mandate

Microsoft filed a petition for a writ of mandate, asking the Court of Appeal to address these critical issues that no Court of Appeal had yet resolved. (Pet. pp. 38-39.) As Microsoft highlighted, writ review was necessary because of the ongoing and irreparable nature of Microsoft's injury in being denied its constitutional right to speak. (Pet. pp. 39-40) and Microsoft had no adequate remedy at law, as it could not obtain appellate review of the trial court's order by other means. (Pet. p. 40.)

[3] The court's decision appeared driven in part by respect for Detective [redacted]. (Vol. II, Ex. 15, p. 356:10-15 ["I have the highest regard for Detective [redacted] having worked with him … I even told Mr. Porter about his [redacted] [redacted] [redacted]."].)

The Reporters Committee for Freedom of the Press, the First Amendment Coalition, and Google LLC filed amicus briefs in support of Microsoft's petition. As the first two organizations explained, overbroad secrecy orders threaten members of the news media's "acute interest in maintaining the confidentiality of data on the cloud." (Amicus Curiae Br. of Reporters Committee for Freedom of the Press and the First Amendment Coalition in Support of Microsoft Corporation's Petition for Writ of Mandate, pp. 8-9.) And Google explained that it has been routinely subjected to CalECPA gag orders, many of which are plainly overbroad—including "where the targeted user was already aware of the investigation," or where "the enterprise itself was not under investigation and there was no basis to believe that a corporate officer, once notified of the warrant, would take any action to compromise the investigation." (Amicus Curiae Br. of Google LLC in Support of Pet'r Microsoft Corp., p. 14.)

The Court of Appeal summarily denied Microsoft's petition on July 18, 2025. Its order stated that Microsoft "failed to demonstrate a prima facie case entitling it to extraordinary appellate relief," providing no further explanation. (Order p. 1.)

REASONS THE COURT SHOULD GRANT REVIEW

A. California Courts Need Guidance On The Standards For CalECPA Secrecy Orders.

This Court should grant Microsoft's petition for review to provide critical guidance on the standards trial courts must apply in assessing CalECPA secrecy orders. Although CalECPA is a decade old, no appellate court has issued any decision clarifying when the secrecy orders contemplated by the statute are appropriate.

This Court's direction is sorely needed given the prevalence of such secrecy orders. Indeed, *thousands* of CalECPA warrants issue each year, most of which are accompanied by broad secrecy orders barring cloud services providers from speaking. According to the California Department of Justice's data on electronic search warrant notifications, law enforcement issued 2,006 CalECPA warrants in 2024 alone—and 1,255 of those warrants incorporated secrecy orders.[4] Of the 1,071 warrants recorded in 2025 to date, 653 have imposed secrecy orders.[5]

[4] (Cal. Dep't of Justice, Electronic Search Warrant Notifications Data Set – Reported in 2024, available at https://data-openjustice.doj.ca.gov/sites/default/files/dataset/2025-06/2024_calecpa_data.csv (last visited July 25, 2025).)

[5] (Cal. Dep't of Justice, Electronic Search Warrant Notifications Data Set – Reported in 2025, available at https://data-openjustice.doj.ca.gov/sites/default/files/dataset/2025-06/2025_calecpa_data.csv (last visited July 25, 2025).)

These issues are important for businesses throughout California, not just cloud services providers like Microsoft. When law enforcement obtains a business's data from its cloud services provider in this manner, the business does not know about and cannot assert its interests with respect to that access. The growing use of CalECPA warrants only increases these concerns.

This Court should use this opportunity to make two fundamental propositions clear. *First*, CalECPA requires the government to provide *a factual basis* that could justify imposing the full breadth of any secrecy order, and the court reviewing an application for such an order must make an independent determination that the government's evidence satisfies its burden. (See *In Re Sealed Case*, *supra*, 2025 WL 2013687 at p. *5.) *Second*, even if CalECPA did not require the government to bear this burden, both the First Amendment to the U.S. Constitution and Article I, Section 1 of the California Constitution would. CalECPA secrecy orders must satisfy strict scrutiny, and they are therefore inappropriate where a less restrictive alternative—such as permitting a cloud services provider to give limited information about the existence of a warrant to its customer, where that customer is not the target of the investigation—will suffice.

1. The Secrecy Order Violates CalECPA.

The secrecy order here flies in the face of CalECPA's text and purpose. "[T]he fundamental purpose of CalECPA[] is to protect the privacy interests of owners and authorized users in their electronic devices and electronic information." (*People v.*

Clymer (2024) 107 Cal. App. 5th 131, 141.) CalECPA thus generally requires notice to a subscriber, like [redacted] here, when law enforcement seeks their information. (Pen. Code, § 1546.2, subd. (a)(1).) The statute authorizes delaying notice—and gagging a cloud service provider—only if the court determines the government has made a showing of a "reason to believe" that notification may cause certain specified adverse results: "Danger to the life or physical safety of an individual"; "Flight from prosecution"; "Destruction of or tampering with evidence"; "Intimidation of potential witnesses"; or "Serious jeopardy to an investigation or undue delay of a trial." (*Id.* §§ 1546.2, subd. (b)(1), 1546, subd. (a).)The *court*, not law enforcement, must make this determination.

But the trial court here did not identify any cognizable "reason to believe" that notification "may have an adverse result," as the statute requires. (Pen. Code, § 1546.2, subd. (b)(1).) Rather, with Detective [redacted] affidavit accompanying the warrant before it, the court initially *agreed* with Microsoft that limited notice to a specified individual at [redacted] of the existence of the warrant would pose no apparent threat to the City's ongoing investigation. The court then reversed course and rejected Microsoft's motion solely because Detective [redacted] refused to agree to this slight modification. The court neither found nor suggested that any evidence before it indicated that such a limited disclosure would have any of CalECPA's specified adverse results. Instead, it speculated that Detective [redacted] may have "more information potentially than was contained in the search warrant affidavit" he had submitted. (Vol. II, Ex. 15, p. 356:21-25.)

In these respects, the trial court's reasoning directly conflicts with the approach the D.C. Circuit held federal courts must adhere to under the SCA, CalECPA's federal analogue. In *In Re Sealed Case*, 2025 WL 2013687, the D.C. Circuit held a SCA secrecy order invalid because the issuing court failed to hold the government to its burden to establish a "reason to believe" one of the factors supporting a secrecy order actually existed. (*Id.* at p. *5.) There, the lower court had issued a secrecy order that prohibited disclosure related to any subpoenas the government issued in connection with its investigation "so long as the *government* decided that disclosure would risk one of the harms specified in the Act." (*Id.* at p. *1.) As the Court of Appeals held, by authorizing secrecy in these broad strokes, the issuing court had impermissibly "outsourced to the government the very evaluation that Congress assigned to the court." (*Id.* at p. *5.) The issuing court accordingly "did not make the required finding before issuing these orders and thus did not conform to [the SCA]." (*Ibid.*)

The trial court's decision here reflects the same fundamental error. Although the court referenced the statutory factors that might preclude disclosure, it did not and could not find that the City had demonstrated that providing limited notice of the type Microsoft proposed would have any adverse effect. Instead, the court speculated that Detective [redacted] may have "more information potentially than was contained in the search warrant affidavit" underlying the secrecy order. (Vol. II, Ex. 15, p. 356:21-25.) The court thus deferred to the City's mere assertion of a need for secrecy, failing to hold the City to its burden of actually *supporting* that claim and "outsource[ing] to the government the very evaluation that [the Legislature] assigned to the court." (*In Re Sealed Case*, *supra*, 2025 WL 2013687at p. *5.)

Indeed, the City did not come close to meeting its burden in any submission to the trial court. Microsoft assumes that the City has shown that informing the *target* of the City's investigation could result in such adverse effects. But the gag order also restricts Microsoft from informing anyone at [redacted] of even the fact of the warrant—even, for example, [redacted]. And the City presented no evidence that could support the conclusion that informing anyone at [redacted] would have any of the specified adverse effects that CalECPA requires before a court imposes such a secrecy order.

The only evidence in the record is to the contrary. [redacted] has no apparent interest in interfering with the LAPD's investigation. If anything, the interests of [redacted] and law enforcement align, as both seek to protect [redacted] from the target of the investigation. The crime under investigation does not implicate corporate wrongdoing or misconduct by [redacted]'s leadership, but rather [redacted]. (Vol. I, Ex. 2, pp. 38-43, 86-99.) [redacted] also has a sophisticated legal department and compliance infrastructure designed to respond to sensitive investigations. (Vol. I, Ex. 2, pp. 168-170.) Microsoft thus proposed several possible candidates for notification. (Vol. I, Ex. 1, pp. 21-22.) The City did not even attempt to show that informing any of the candidates of the fact of the warrant would somehow undermine the investigation.

The Court should grant review and join the D.C. Circuit in holding that that courts must make an independent determination of the government's need for secrecy based on actual evidence. The Legislature designed CalECPA to be *more* privacy-protective than its federal counterpart. California courts should not defeat the Legislature's intent by interpreting it otherwise.

2. The Secrecy Order Violates Microsoft's Speech Rights Under The California And Federal Constitutions.

Review is also needed to vindicate the fundamental constitutional rights that such overbroad secrecy orders violate.

a. Secrecy Orders Are Subject To Strict Scrutiny.

"Nondisclosure orders implicate two disfavored types of speech restrictions: prior restraints and content-based restrictions." (*In re Sealed Case* (D.C. Cir. 2023) 77 F.4th 815, 829.) For both reasons, secrecy orders are subject to strict scrutiny—as the City conceded. (Vol. II, Ex. 13, p. 282.)

First, secrecy orders are prior restraints because they "suppress[] speech … in advance of its [actual] expression." (*Long Beach Area Peace Network v. City of Long Beach* (9th Cir.

2009) 574 F.3d 1011, 1023.) Here, the order bars Microsoft from speaking to its customer—[redacted]—about the government’s request for and seizure of the customer’s data, preemptively forbidding Microsoft’s otherwise lawful expression. Court orders like this one “that actually forbid speech activities[] are classic examples of prior restraints.” (*Alexander v. United States* (1993) 509 U.S. 544, 550.) Courts have consistently reached that conclusion with respect to analogous secrecy orders under the federal SCA. (See, e.g., *Matter of Search Warrant for [redacted].com* (2017) 248 F.Supp.3d 970, 980 [collecting cases].)

Courts apply strict scrutiny to prior restraints because they constitute “the most serious and the least tolerable infringement” on our freedoms of speech and press. (*Neb. Press Assn. v. Stuart* (1976) 427 U.S. 539, 559; see *Matter of Subpoena 2018R00776* (3d Cir. 2020) 947 F.3d 148, 155-156; *Matter of Search of Info. Associated With Specified E-Mail Accts.* (E.D.N.Y. 2019) 470 F.Supp.3d 285, 291 [applying strict scrutiny when reviewing secrecy order under the SCA].) Any prior restraint thus bears “a ‘heavy presumption’ against its constitutional validity[,]” and the government “carries a heavy burden of showing justification for the imposition of such a restraint.” (*Neb. Press*, *supra*, 427 U.S. at p. 558 [citation omitted].) And the California Constitution is *more* protective of free speech rights than the federal Constitution: California courts require “‘extraordinary circumstances’ before a prior restraint may be imposed." (*Molinaro v. Molinaro* (2019) 33 Cal.App.5th 824, 832 [citation omitted].)

Second, secrecy orders are content-based restrictions because they "effectively preclude speech on an entire topic"—namely, the underlying warrant. (*In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders* (S.D. Tex. 2008) 562 F.Supp.2d 876, 881 [addressing analogous SCA].) "[A] speech regulation is content based if [it] applies to particular speech because of the topic discussed or the idea or message expressed." (*Reed v. Town of Gilbert* (2015) 576 U.S. 155, 171.) The secrecy order here bars Microsoft from discussing with its customer—the audience to whom the speech is most germane—the government's seizure of the customer's data, and thus it is content-based. (See *In re Sealing*, *supra*, 562 F.Supp.2d at p. 881.) Like a prior restraint, "[a] content-based restriction on speech is presumptively invalid[,]" (*Eclipse Enters., Inc. v. Gulotta* (2d Cir. 1997) 134 F.3d 63, 67), and may stand only if it survives strict scrutiny. (See *Matter of Search of Info.*, *supra*, 470 F.Supp.3d at p. 290 [applying strict scrutiny when reviewing SCA secrecy order].)

b. The Secrecy Order Cannot Survive Strict Scrutiny.

A secrecy order like the one here cannot withstand that searching inquiry. Under strict scrutiny, the government must prove it has narrowly tailored its speech restriction to promote a compelling government interest using the least restrictive means. (See *United States v. Playboy Ent. Grp.* (2000) 529 U.S. 803, 813.) "When a plausible, less restrictive alternative is offered," the government must "prove that the alternative will be ineffective to achieve its goals." (*Id.* at p. 816.) The trial court failed to hold the City to that burden here.

The City's sole professed interest is in maintaining "the investigation's secrecy," as the investigation "is open, ongoing, and involves significant crimes." (Vol. II, Ex. 13, pp. 282-283.) That is true for virtually every investigation, and these facts do not show the risk to any compelling interest at issue here. Microsoft does not dispute that the City may have a compelling interest in ensuring that certain parties—in particular, the *target* of the investigation—do not learn of the warrant. But as detailed above, the City failed to meet its burden of showing that to achieve its goal, it is necessary to maintain the secrecy order's broader ban on informing *anyone* at [redacted]. (*Supra* pp. 23-24.)

That failure dooms the secrecy order. Given Microsoft's proposed plausible, less restrictive alternative of notifying a trustworthy contact at [redacted] of the existence of the warrant (but not the account sought), the City was required to "prove that the alternative[s] will be ineffective to achieve its goals." (*Playboy*, *supra*, 529 U.S. at p. 816.) While the City argued generally that notification "could interfere with the investigation" (Vol. II, Ex. 13, p. 284), it provided no information to support this statement—much less the "hard evidence" strict scrutiny demands. (*Playboy*, *supra*, 529 U.S. at p. 819; see also *Landmark Commc'ns, Inc. v. Virginia* (1978) 435 U.S. 829, 841 [concluding the government failed to meet its burden where it "offered little more than assertion and conjecture to support its claim"].) To the contrary, the City effectively conceded at the initial hearing that Microsoft's proposed compromise *was* effective.

In later deferring to the City's contrary assertions and forgiving its failure to provide any factual support, the trial court abdicated its critical role of ensuring that the government justify a restraint on speech. Instead, the court relied on speculation that Detective [redacted] might have some as-yet-undisclosed reason to believe that informing [redacted] would be problematic. (Vol. II, Ex. 15, p. 356:21-25.) That has things backwards. It is the government's obligation to provide *evidence* to support its restriction on Microsoft's speech. (*Playboy*, *supra*, 529 U.S. at p. 819.) A court cannot presume that, despite the failure to provide any such evidence, the government must nevertheless have a basis for gagging Microsoft. (See, e.g., *id*. at pp. 822-823 [rejecting "anecdote and supposition" as inadequate "proof" to justify restriction]; see also *Landmark Commc'ns*, *supra*, 435 U.S. at p. 841 [no basis for restraint when government "offered little more than assertion and conjecture to support its claim"].) This Court's review is needed to make clear that this sort of speculation cannot support such a prior restraint.

B. This Case Is An Excellent Vehicle For The Court To Address These Issues.

This case squarely presents these important issues regarding the permissible scope of CalECPA secrecy orders. These questions are unlikely to come before this Court in any better vehicle. Indeed, by their very nature, CalECPA secrecy orders tend to evade appellate review. The statute requires that they be time-limited to 90 days unless renewed. (Pen. Code, § 1546.2, subd. (b)(1).) Moreover, a cloud services provider to which a warrant is directed will not be a party to the criminal case that may result from the investigation, and thus could never appeal from it. (See Pen. Code, §§ 1237-1238 [limiting parties who can appeal in criminal cases to the state and defendant]; *People v. Green* (2004) 125 Cal.App.4th 360, 378 [only "the People and the defendant" are parties to criminal proceedings, and third parties may not seek relief through a typical appeal].)

Although review via writ petition is theoretically possible, no party has yet secured such relief in the decade since the Legislature enacted CalECPA. The Court of Appeal's summary denial of Microsoft's petition ensures that there will remain no governing precedent on these critical issues unless this Court acts. Microsoft's speedy challenge to the secrecy order here brings the issue before the Court as quickly as possible, and its petition presents only the straightforward issues outlined above.

Even if the gag order expires on July 31 as scheduled, the need for this Court's review remains. That is because the case "poses an issue of broad public interest that is likely to recur." (*Edelstein v. City & County of San Francisco* (2002) 29 Cal.4th 164, 172, quoting *In re William M.* (1970) 3 Cal.3d 16, 23, 89.) This Court has thus "frequently exercised [its] discretion" to review such constitutional issues, regardless whether intervening events have rendered the issues moot. (*Ibid.*; cf. *In*

Re Sealed Case, *supra*, 2025 WL 2013687, at p. *3 [reviewing expired secrecy orders under federal exception to mootness because the orders’ duration was “too fleeting for litigation to run its course” and the cloud services provider “reasonably expect[s] to face another nondisclosure order”].)

Such review is especially warranted here given the nature of the constitutional rights at issue. The loss of the right to speak “‘for even minimal periods of time, unquestionably constitutes irreparable injury.’” (*Ketchens v. Reiner* (1987) 194 Cal.App.3d 470, 480, quoting *Elrod v. Burns* (1976) 427 U.S. 347, 373.) Without this Court’s intervention, the many secrecy orders imposed each year may cause irreparable harms that nevertheless escape review. The Court should ensure that trial courts hold the government to its burden and prevent similar injuries in the future.

CONCLUSION

For the reasons above, Microsoft requests that the Court grant this petition for review.

Dated: July 28, 2025 DAVIS WRIGHT TREMAINE LLP

By: */s/ James R. Sigel*
James R. Sigel
Attorneys for Petitioner
Microsoft Corp.

CERTIFICATE OF WORD COUNT

Pursuant to Rule 8.204(c) of the California Rules of Court and in reliance on the word count of the computer program used to prepare this brief, counsel certifies that this petition was produced using at least 13 point font and contains 5903 words.

Dated: July 28, 2025

/s/ James R. Sigel
James Sigel

PROOF OF SERVICE

I am employed in the County of San Francisco, State of California. I am over the age of 18 and not a party to the within action. My business address is Davis Wright Tremaine, LLP, 50 California Street, 23rd Floor, San Francisco, CA 94111.

On July 28, 2025, I served the following document(s):

MICROSOFT'S PETITION FOR REVIEW

as follows:

SEE ATTACHED SERVICE LIST

☒ (***VIA TRUEFILING***) – On July 28, 2025 I electronically served a true and correct electronic copy of said documents via TrueFiling.

☒ (***VIA FEDEX OVERNIGHT DELIVERY***) and by sealing the envelope and placing it for collection and delivery by ***FedEx*** overnight service with delivery fees paid or provided for in accordance with ordinary business practices.

I declare under penalty of perjury, under the laws of the State of California, that the foregoing is true and correct.

Executed on July 28, 2025, at San Francisco, California.

Amanda Henderson
Print Name

Signature

SERVICE LIST

Clerk of the Court of Appeal
Second Appellate District, Division 4
300 S. Spring Street
2nd Floor, North Tower
Los Angeles, CA 90013
Case No. B347381

Service by FedEx

Clerk of the Superior Court
For the Honorable Craig Richman
Los Angeles County Superior Court
Dept. 119
Clara Shortridge Foltz Criminal
Justice Center
210 West Temple Street
Los Angeles, CA 90012
Case No. 25CJGP00165

Service by FedEx

Hasmik Badalian Collins
Deputy City Attorney
Los Angeles City Attorney's Office
Public Safety General Counsel
Division
200 N. Main St., 8th Floor
Los Angeles, CA 90012
Main Line: (213) 978-8380
hasmik.collins@lacity.org

Counsel for Real Party in Interest City Of Los Angeles

Service by TrueFiling and FedEx

Hydee Feldstein Soto
City Attorney
Carlos de la Guerra
Assistant City Attorney
Wayne Song
Supervising Asst. City Attorney
Soraya C. Kelly
Deputy City Attorney
Los Angeles City Attorney's Office

200 N. Main St., 8th Floor
Los Angeles, CA 90012
Main Line: (213) 978-8380
hydee.feldsteinsoto@lacity.org
carlos.delaguerra@lacity.org
wayne.song@lacity.org
soraya.kelly@lacity.org

The Honorable Craig Richman
Los Angeles County Superior Court
Dept. 119
Clara Shortridge Foltz Criminal
Justice Center
210 West Temple Street
Los Angeles, CA 90012

Respondent

Service by FedEx

ATTACHMENT: COURT OF APPEAL ORDER

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION FOUR

MICROSOFT CORP.,

Petitioner,

v.

SUPERIOR COURT OF LOS ANGELES COUNTY,

Respondent;

CITY OF LOS ANGELES,

Real Party in Interest.

B347381

(Los Angeles County
Super. Ct. No. 25CJGO00165)
(Craig Richman, J.)

ORDER

THE COURT: *

The petition for writ of mandate filed on July 3, 2025, has been read and considered, along with the request for a stay, application to seal, applications to file amicus curiae briefs, and the applications for *pro hac vice* admission of Ambika Kumar and Maryann T. Almeida. The *pro hac vice* applications are granted along with the July 10, 2025 application to file a redacted petition for writ of mandate, as amended pursuant to the July 9, 2025 order, to redact information sealed by the trial court until July 31, 2025.

Because petitioner failed to demonstrate a prima facie case entitling it to extraordinary appellate relief, the petition is denied. Accordingly, the applications to file amicus curiae briefs are denied as well.

Collins

* COLLINS, Acting P.J. TAMZARIAN, J. GARCIA UHRIG, J. **

** Judge of the Los Angeles Superior Court, assigned by the Chief Justice pursuant to article VI, section 6, of the California Constitution.

ATTACHMENT: TRIAL COURT ORDER

Trial court order from conditionally sealed record omitted.