

S286267

**IN THE
SUPREME COURT OF CALIFORNIA**

SNAP, INC., *Petitioner,*

v.

THE SUPERIOR COURT OF SAN DIEGO COUNTY, *Respondent;*

ADRIAN PINA et al., *Real Parties in Interest.*

META PLATFORMS INC., *Petitioner,*

v.

THE SUPERIOR COURT OF SAN DIEGO COUNTY, *Respondent;*

ADRIAN PINA et al., *Real Parties in Interest.*

AFTER A DECISION BY THE COURT OF APPEAL,
FOURTH APPELLATE DISTRICT, DIVISION ONE • CASE NOS. D083446, D083475
SAN DIEGO COUNTY SUPERIOR COURT • DANIEL F. LINK, JUDGE • CASE No. CN429787

**APPLICATION FOR LEAVE TO FILE AMICUS CURIAE BRIEF AND
AMICUS CURIAE BRIEF OF THE CHAMBER OF COMMERCE OF
THE UNITED STATES OF AMERICA IN SUPPORT OF
PETITIONERS SNAP, INC. AND META PLATFORMS INC.**

HORVITZ & LEVY LLP

ERIC S. BOORSTIN (BAR No. 253724)

*BENJAMIN P. COVINGTON (BAR No. 340180)

3601 WEST OLIVE AVENUE, 8TH FLOOR

BURBANK, CALIFORNIA 91505-4681

(818) 995-0800 • FAX: (844) 497-6592

eboorstin@horvitzlevy.com

bcovington@horvitzlevy.com

HORVITZ & LEVY LLP

JEREMY B. ROSEN (BAR No. 192473)

505 SANSOME STREET, SUITE 1550

SAN FRANCISCO, CALIFORNIA 94111-3149

(415) 462-5600 • FAX: (844) 497-6592

jrosen@horvitzlevy.com

ATTORNEYS FOR AMICUS CURIAE
CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA

Document received by the CA Supreme Court.

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	4
APPLICATION FOR LEAVE TO FILE AMICUS CURIAE BRIEF.....	7
AMICUS CURIAE BRIEF	10
INTRODUCTION	10
LEGAL ARGUMENT	12
I. The business model theory contradicts the Stored Communications Act’s statutory text, which assumes that online service providers may access user communications without forfeiting protection.	12
II. The business model theory would be unworkable for courts, providers, and users.....	15
A. Proponents of the business model theory cannot agree on what it means.....	15
B. Several versions of the business model theory would require courts to resolve intractable debates about computer security and business necessity.....	19
C. Other versions of the business model theory would put courts to a false dilemma of deciding whether a business practice benefits the user or the provider, when in fact it benefits both.....	22
III. The business model theory undermines the SCA’s purpose of encouraging businesses’ development and consumers’ use of new communications technologies.....	28
A. The business model theory may mandate that businesses adopt a pay-for-service model.....	28
B. The business model theory would unduly burden providers with discovery requests.	29
IV. The business model theory violates the SCA’s purpose of providing stronger privacy protections than the Fourth Amendment.....	32

Document received by the CA Supreme Court.

CONCLUSION.....36
CERTIFICATE OF WORD COUNT37

Document received by the CA Supreme Court.

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Brawley v. Crosby Research Foundation</i> (1946) 73 Cal.App.2d 103	20
<i>Brown v. Google, LLC</i> (N.D.Cal., Dec. 12, 2022, No. 20-cv-3664-YGR) 2022 WL 17961497	19
<i>Carpenter v. United States</i> (2018) 585 U.S. 296 [138 S.Ct. 2206, 201 L.Ed.2d 507]	33, 34
<i>Epic Games, Inc. v. Apple, Inc.</i> (9th Cir. 2023) 67 F.4th 946	19, 29
<i>Epic Games, Inc. v. Apple Inc.</i> (N.D.Cal. 2020) 493 F.Supp.3d 817	26
<i>Facebook, Inc. v. Superior Court</i> (2018) 4 Cal.5th 1245.....	12, 21, 28, 32
<i>Facebook, Inc. v. Superior Court of San Diego County</i> (2020) 10 Cal.5th 329.....	<i>passim</i>
<i>Gaillard v. Natomas Co.</i> (1989) 208 Cal.App.3d 1250	21
<i>In re Arris Cable Modem Consumer Litigation</i> (N.D.Cal. 2018) 327 F.R.D. 334.....	19
<i>NCAA v. Alston</i> (2021) 594 U.S. 69.....	21
<i>Nunn v. State of California</i> (1984) 35 Cal.3d 616	14
<i>O’Grady v. Superior Court</i> (2006) 139 Cal.App.4th 1423	12, 28, 29, 30, 31
<i>Ohio v. American Express Co.</i> (2018) 585 U.S. 529 [138 S.Ct. 2274, 201 L.Ed.2d 678]	22, 23

<i>Riley v. California</i> (2014) 573 U.S. 373 [134 S.Ct. 2473, 189 L.Ed.2d 430]	34
<i>Smith v. Maryland</i> (1979) 442 U.S. 735 [99 S.Ct. 2577, 61 L.Ed.2d 220]	33, 34
<i>Snap, Inc. v. Superior Court of San Diego County</i> (2024) 103 Cal.App.5th 1031	<i>passim</i>
<i>United States v. Miller</i> (1976) 425 U.S. 435 [96 S.Ct. 1619, 48 L.Ed.2d 71]	33, 34
<i>United States v. Miller</i> (6th Cir. 2020) 982 F.3d 412	25

Statutes

18 U.S.C.	
§ 2702	15
§ 2702(a)	12, 14
§ 2702(b)	12, 14
§ 2702(c)	12, 14
§ 2702(b)(6)	13
§ 2702(b)(8)	14
§ 2702(c)(5)	13, 14
§ 2707(a)	30
§ 2707(e)(1)	30

Rules of Court

Cal. Rules of Court	
rule 8.520(f)(1)	7
rule 8.520(f)(4)	7

Miscellaneous

Amicus Brief, <i>Gilead Sciences, Inc. v. Superior Court</i> (Cal., Nov. 5, 2024, No. S283862) 2024 WL 4834681	8
Amicus Brief, <i>Gonzalez v. Google LLC</i> (U.S., Jan. 19, 2023, No. 21-1333) 2023 WL 375043	8
Amicus Brief, <i>In re Search of Information Associated with Specified E-Mail Accounts</i> (2d Cir., Dec. 22, 2010, Nos. 20-1653, 20-3945) 2020 WL 7908208	8

Amicus Brief, <i>Madrigal v. Hyundai Motor America</i> (Cal., July 26, 2024, No. S280598) 2024 WL 5279377	8
Amicus Brief, <i>Salazar v. Paramount Global</i> (6th Cir., Feb. 2, 2024, No. 23-5748) 2024 WL 519870	8
Crane, <i>Defining Relevant Markets in Digital Ecosystems</i> (2024) 7 Journal of Law & Innovation 10	23
Interactive Advertising Bureau, <i>The Free and Open Ad-Supported Internet</i> (2024) < https://tinyurl.com/447ccf3n > [as of Feb. 18, 2025]	26, 27
Lebow, <i>Advertising Makes Up The Lion’s Share of Mobile App Revenues</i> (Sept. 25, 2023) eMarketer < https://tinyurl.com/2e3x29c3 > [as of Feb. 18, 2025]	26
Marchese, <i>Debunking the “Big Is Bad” Bogeyman</i> (2020) 28 Geo. Mason L.Rev. 1.....	23, 24
Meta, <i>Government Requests for User Data</i> , < https://tinyurl.com/39cjpekr > [as of Feb. 7, 2025]	30, 31
Niels & Ralston, <i>Two-Sided Market Definition: Some Common Misunderstandings</i> (2021) 17 European Competition Journal 118.....	23
Rest.2d Contracts, § 79, com. c.....	20
Sen.Rep. No. 99-541, 2d Sess. (1986).....	32

APPLICATION FOR LEAVE TO FILE AMICUS CURIAE BRIEF

Pursuant to California Rules of Court, rule 8.520(f)(1), the Chamber of Commerce of the United States of America (the “Chamber”) requests permission to file the attached amicus curiae brief in support of petitioners Snap, Inc. and Meta Platforms Inc.¹

The Chamber is the world’s largest business federation. It represents approximately 300,000 direct members and indirectly represents the interests of more than 3 million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files amicus curiae briefs in cases, like this one, that raise issues of concern to the Nation’s business community.

The Chamber’s members include some of the world’s leading technology companies. Billions of people rely daily on these companies’ search engines, email services, social networks, dating sites, smartphones, cloud storage, and internet-based

¹ No party or counsel for a party in the pending appeal authored this proposed brief in whole or in part or made a monetary contribution intended to fund the preparation or submission of the proposed brief. No person or entity other than amicus, its members, or its counsel made a monetary contribution intended to fund the preparation or submission of the proposed brief. (See Cal. Rules of Court, rule 8.520(f)(4).)

devices and applications. Users entrust these technology companies with some of their most important information and communications. Given this trust, the companies continuously work to secure their users' privacy and safety.

The Chamber's interest in this case arises out of concern for the important privacy interests of the individuals who use online services, the ability of technology companies to implement safety and content-moderation policies, and the impact on technology companies of the high cost and burden of responding to subpoenas from third parties.


The proposed amicus brief explains how the theory advanced by the Court of Appeal, which overturns the longstanding application of the Stored Communications Act, is unworkable, inconsistent with that statute's text and purpose, and unduly burdensome both to individuals and the technology companies responsible for safeguarding their private data.

The Chamber regularly files amicus briefs in cases that impact the technology industry. (See, e.g., Amicus Brief, *Salazar v. Paramount Global* (6th Cir., Feb. 2, 2024, No. 23-5748) 2024 WL 519870; Amicus Brief, *Gonzalez v. Google LLC* (U.S., Jan. 19, 2023, No. 21-1333) 2023 WL 375043; Amicus Brief, *In re Search of Information Associated with Specified E-Mail Accounts* (2d Cir., Dec. 22, 2010, Nos. 20-1653, 20-3945) 2020 WL 7908208.) The Chamber also regularly files amicus briefs before this Court. (See, e.g., Amicus Brief, *Gilead Sciences, Inc. v. Superior Court* (Cal., Nov. 5, 2024, No. S283862) 2024 WL 4834681; Amicus

Brief, *Madrigal v. Hyundai Motor America* (Cal., July 26, 2024,
No. S280598) 2024 WL 5279377.)

February 24, 2025

HORVITZ & LEVY LLP
JEREMY B. ROSEN
ERIC S. BOORSTIN
BENJAMIN P. COVINGTON

By: 
Benjamin P. Covington

Attorneys for Amicus Curiae
**CHAMBER OF COMMERCE OF THE
UNITED STATES OF AMERICA**

Document received by the CA Supreme Court.

**AMICUS CURIAE BRIEF OF THE CHAMBER OF
COMMERCE OF THE UNITED STATES OF AMERICA
IN SUPPORT OF PETITIONERS SNAP, INC. AND
META PLATFORMS INC.**

INTRODUCTION

The Court of Appeal’s adoption of the “business model theory” eliminates privacy protections long afforded by the Stored Communications Act (SCA) to online service providers and their billions of users. That theory—if it can fairly be described as one—requires that an online service provider forfeit its users’ SCA protections if it can access its users’ communications for some still-unspecified set of purposes beyond strictly transmitting or storing them.

Depending on which of the many versions of the theory might be adopted, companies would lose SCA protections if they engage in commonplace practices like scanning communications to detect and report child pornography, implementing content-moderation policies to remove harassing or otherwise objectionable content, and generating revenue on a platform offered for free by facilitating user-tailored advertising. Online service providers should not have to choose between the SCA’s protections and these ubiquitous practices. And every tool of statutory construction makes clear that the SCA does not require them to.

First, the business model theory contradicts the SCA’s text. The theory treats communications as a black box that can never be accessed by online platforms except for simple

transmission and storage. Yet the SCA itself authorizes online service providers to report child pornography and ongoing emergencies—authorizations that necessarily assume other reasons for provider access.

Second, the business model theory cannot be applied in a principled manner. Five years after the concurrence in *Facebook, Inc. v. Superior Court of San Diego County* (2020) 10 Cal.5th 329 (*Touchstone*) suggested the theory, its proponents still have not agreed on a test to apply it. The version of the theory that would bar *all* access cannot be squared with the SCA’s contemplation of provider access. The versions that allow *some* access lack any grounding in the SCA’s text and give no meaningful guidance on when the SCA would apply. Courts would wade into intractable debates: whether, for example, access is “reasonably necessary” for computer “integrity.” Or courts would resolve a false dilemma: whether, for example, access is purely for the user’s benefit or purely for the platform’s benefit.

Adoption of the theory guarantees that courts would reach inconsistent results. Providers would be hard-pressed to predict whether their terms of service forfeit SCA protection. And users, previously safe to assume SCA coverage for their communications, would be left guessing as to when their most private communications might be revealed.

Third, the business model theory would undermine the SCA’s purpose of encouraging the development and use of new communications technologies. The theory would either saddle online platforms with significant compliance costs or, as the

Touchstone concurrence candidly admitted, may mandate that platforms “revert to an old-school pay-for-service business model” if they would like to keep their SCA coverage.

Fourth, the business model theory would flip on its head the SCA’s goal of furnishing broader privacy protections than the Fourth Amendment. The Court of Appeal justified its adoption of the business model theory by categorically concluding that users have no expectation of privacy in information they share with a third-party provider. But the Supreme Court recently rejected this exact reasoning in a Fourth Amendment case involving information shared with a cell-service provider. The business model theory would therefore produce the anomalous result of making the SCA narrower than the Fourth Amendment—despite Congress’s intention to do just the opposite.

LEGAL ARGUMENT

I. The business model theory contradicts the Stored Communications Act’s statutory text, which assumes that online service providers may access user communications without forfeiting protection.

The SCA bars providers of electronic communications services or remote computing services from knowingly divulging user information or contents unless doing so falls within one of nine enumerated exceptions. (18 U.S.C. § 2702(a)–(c).) Congress’s purpose in enacting the SCA was threefold: “(1) protecting the privacy expectations of citizens, (2) recognizing the legitimate needs of law enforcement, and (3) encouraging the use and development of new technologies.” (*Facebook, Inc. v. Superior Court* (2018) 4 Cal.5th 1245, 1263 (*Hunter*); see *O’Grady*

v. Superior Court (2006) 139 Cal.App.4th 1423, 1444–1445 (O’Grady) [“Congress thus sought not only to shield private electronic communications from government intrusion but also to encourage ‘innovative forms’ of communication by granting them protection against unwanted disclosure *to anyone*”].)

The business model theory suggests that an online provider forfeits its users’ SCA protections if it can access communications for “‘other purposes’” besides simply transmitting or storing them. (*Touchstone, supra*, 10 Cal.5th at pp. 370–373 (conc. opn. of Cantil-Sakauye, C.J.); *Snap, Inc. v. Superior Court of San Diego County* (2024) 103 Cal.App.5th 1031, 1062–1064 (Pina).) In other words, the theory interprets the SCA to apply to communications only if those communications are a black box that *cannot* be accessed except when doing so is strictly necessary for transmission and storage.

But as Snap and Meta explain, that interpretation cannot be squared with the SCA’s text, which contemplates that providers *can* access communications for other reasons. (Meta OBOM 25–28; Snap OBOM 21, 49–50; Meta RB 7, 13–15; Snap RB 22.) Multiple exceptions to the SCA’s nondisclosure bar are content-based, meaning a provider can make a disclosure under them only if it had previously accessed the communication’s content. The SCA, for example, authorizes online providers to report instances of child pornography to the National Center for Missing and Exploited Children. (18 U.S.C. § 2702(b)(6), (c)(5).) It also authorizes online providers to report both “the contents of a communication” and noncontent user information to

government authorities when they have a good-faith belief “that an emergency involving danger of death or serious physical injury to any person requires disclosure.” (*Id.*, § 2702(b)(8), (c)(5).)

No proponent of the business model theory has explained how that theory can coherently interpret section 2702(a)’s, disclosure bar to require absolute nonaccess when at least two of section 2702(b) and (c)’s exceptions to that bar could apply only if a provider can access communications.

The *Touchstone* concurrence and the Court of Appeal’s opinion acknowledged that there are exceptions to the SCA’s nondisclosure bar, but they overlook how those exceptions conflict with the business model theory’s baseline assumption of nonaccess. (*Touchstone, supra*, 10 Cal.5th at p. 363, fn. 4 (conc. opn. of Cantil-Sakauye, C.J.) “[t]he Act lists exceptions”]; *Pina, supra*, 103 Cal.App.5th at p. 1060 [the SCA “[l]ists the exceptions to the general prohibition[]”].) The People offer only the unexplained contention that attempting to harmonize the scope of the nondisclosure bar with its exceptions is somehow “devious” and “obviously flawed” (People ABOM 42), even though this Court has explained that “the various parts of [a] statutory enactment must be harmonized by considering [a] particular clause in the context of the whole statute” (*Nunn v. State of California* (1984) 35 Cal.3d 616, 625).

Pina, for his part, recognizes the import of the SCA’s exceptions to the business model theory. He concedes that the exceptions to the SCA establish that *some* access is allowed, but he argues that Meta and Snap engage in the wrong kinds of

access. (See Pina ABOM 38–39 [arguing “for-profit” access is not “the same as the previously included exceptions found in section 2702”].) But this watered-down version of the business model theory fares no better as an interpretation of the SCA. As explained below, the attempts by Pina and others to craft a version of the business model theory that allows some types of access but not others are gerrymandered tests untethered to the SCA’s text and would be entirely unworkable in practice.

II. The business model theory would be unworkable for courts, providers, and users.

A. Proponents of the business model theory cannot agree on what it means.

Unmoored from any statutory language, proponents of the business model theory have proposed about a dozen different tests for how to apply it. Whichever version the theory were to take, it would fail to provide courts, platforms, and users with any meaningful guidance on when the SCA protects user communications from unwanted disclosure. Some versions would require courts to wade into intractable debates they are ill-equipped to handle: whether, for example, a provider’s access is “excessive” or “reasonably necessary.” Others would require courts to resolve false dilemmas: whether, for example, a type of access benefits the consumer versus the business. This inability to articulate a workable test shows just how far afield from the SCA’s text the theory is. It also highlights just how counter to the SCA’s purposes the theory runs. In passing a law to safeguard businesses’ and users’ confidence in innovative

communications platforms, Congress could not have possibly wanted the application of the SCA’s privacy protections to turn on the results of such hard-to-predict and subjective inquiries.

Concurring in *Touchstone*, then-Chief Justice Cantil-Sakauye suggested, at a minimum, five versions of the business model theory. The concurrence mainly articulated a hair-trigger test for the theory under which SCA protection is lost if a provider can access communications for *any* “‘other purposes’” besides simple transmission and storage. (*Touchstone, supra*, 10 Cal.5th at p. 370 (conc. opn. of Cantil-Sakauye, C.J.)) But elsewhere, the concurrence—without acknowledging it—suggested a version of the theory that requires assessing a provider’s subjective intent: whether the provider has other “*motivating purposes*” for its access. (*Id.* at p. 371, emphasis added.) Still elsewhere, the concurrence offered three versions of the theory that would allow *some* access:

- Whether a provider “conducts itself in ways that go far beyond what Congress contemplated in 1986 that any [provider] would undertake” (*id.* at p. 368);
- Whether a provider’s access “goes substantially beyond” what is “necessary” to provide transmission or storage (*id.* at p. 370); and
- Whether a provider’s access is “reasonably necessary to ensure the safety and integrity of any computer system” (*id.* at p. 372, fn. 14).

The Court of Appeal similarly offered a range of tests for applying the business model theory without acknowledging it was doing so. Like the *Touchstone* concurrence, the opinion at certain points suggested a hair-trigger test under which SCA protection is lost if a provider has any “ability to access and use” communications. (*Pina, supra*, 103 Cal.App.5th at pp. 1038–1039, 1065.) But at other points, the opinion concluded that SCA protection is lost only when a provider’s access is for its “own business purposes” or its “own profit-driven purposes.” (*Id.* at pp. 1038, 1062–1063.) The opinion did not explain what it meant by those terms, but it assumed that accessing communications to identify “wrongdoing” and remove “illicit content” is not a business purpose. (*Id.* at pp. 1064–1065.)

Before this Court, Pina and the People suggest even more possibilities—again without explaining how any of their proposed tests are based on the SCA’s text. Pina at times echoes the *Touchstone* concurrence and the Court of Appeal’s no-access-at-all test. (See Pina ABOM 34 [“access and use”].) Elsewhere, Pina elaborates on the Court of Appeal’s “business purposes” or “profit” tests—arguing that SCA protection is not forfeited when access is for “administrative and safety services that are not for the profit of the company and do not destroy the protections of the SCA.” (Pina ABOM 39; see Pina ABOM 2 [“own profit and business purposes”], 36 [“own business purposes”], 38 [“for-profit access”].) And still elsewhere, Pina suggests a couple tautological approaches: The SCA’s privacy protections do not apply when a provider can access communications “for purposes beyond the

scope” of the SCA, or when access “violate[s] the customer’s privacy” afforded by the SCA. (Pina ABOM 5, 25.)

The People similarly float a range of approaches. Like Pina, the People suggest that SCA protection depends on whether a particular access is “on ‘behalf of’ [a provider] []rather than the customer.” (People ABOM 32.) But mainly, the People would implement the business model theory by having courts make value judgments about the degree of access, asking:

- Whether a provider enjoys an “excessive license” over user communications (People ABOM 12–13, 32, 43); or
- Whether a provider’s access goes “far beyond what is required” or “what is necessary” (People ABOM 13, 36).

The hair-trigger version of the business model theory that bars *all* access can’t be squared with the SCA’s exceptions, which assume provider access. (*Ante*, section I.A.) And the remaining tests that allow *some* access read like attempts to fashion a common law rule. Those tests might reflect how the theory’s proponents would, in the first instance, balance privacy rights against litigants’ interests in access. But they have nothing to do with the task before this Court: interpreting the statutory text that the United States Congress actually adopted in the SCA. Worse yet, each version of the theory that has been proposed would be entirely unworkable.

B. Several versions of the business model theory would require courts to resolve intractable debates about computer security and business necessity.

Consider the *Touchstone* concurrence’s suggestion that a platform might retain SCA protection if its access is “reasonably necessary to ensure the safety and integrity of any computer system.” (*Touchstone, supra*, 10 Cal.5th at p. 372, fn. 14 (conc. opn. of Cantil-Sakauye, C.J.).)

To begin, the intricacies of computer security are likely beyond the knowledge of generalist judges. Indeed, courts have routinely treated that subject as one requiring expert testimony. (See, e.g., *Epic Games, Inc. v. Apple, Inc.* (9th Cir. 2023) 67 F.4th 946, 992 (*Epic Games*) [describing testimony of computer security expert]; *Brown v. Google, LLC* (N.D.Cal., Dec. 12, 2022, No. 20-cv-3664-YGR) 2022 WL 17961497, at p. *9 [nonpub. opn.] [qualifying “security technologist” with graduate degree in computer science to offer “data and privacy opinions”]; *In re Arris Cable Modem Consumer Litigation* (N.D.Cal. 2018) 327 F.R.D. 334, 363 [qualifying expert “who holds a bachelor’s degree in mathematics . . . and Ph.D. in computer science” in “the area of computer networking”].)

Beyond that, “safety” and “integrity” are not one-size-fits-all concepts that universally apply to “any computer system.” (*Touchstone, supra*, 10 Cal.5th at p. 372, fn. 14 (conc. opn. of Cantil-Sakauye, C.J.).) Businesses may reasonably take different views on what they—and their users—believe is necessary for platform integrity. Some businesses might conclude that

automated malware scans meet their security needs. Others might choose to also incorporate human review aimed at preventing fraud by detecting social-engineering attacks. The business model theory would require courts to definitively resolve which components of security apply to “any computer system,” even though businesses have reasonable and good-faith differences about what’s necessary for security.

Next, consider the “excessive license” test that the People propose. That test would require courts to decide whether the access a provider has is “excessive” in relation to the purported “consideration” its users provide in the form of their online communications. (People ABOM 12–13, 32, 43.)

The contours of this test are far from clear, but it would seemingly make the SCA’s application depend on a task that courts both in California and across the country have rejected: weighing the wisdom or value of a private agreement. It is a hornbook contracts rule that “[t]he law does not weigh the quantum of the consideration.” (*Brawley v. Crosby Research Foundation* (1946) 73 Cal.App.2d 103, 112.) That is because parties to an agreement “are thought to be better able than others to evaluate the circumstances of particular transactions” and, “[i]n any event, they are not ordinarily bound to follow” the valuation of a court. (Rest.2d Contracts, § 79, com. c, p. 201.)

More generally, the versions of the business model theory that inquire into “necessity,” the degree of access, and “excessiveness” diverge from courts’ reluctance to second-guess a business’s judgment of what’s required for its success. (See, e.g.,

NCAA v. Alston (2021) 594 U.S. 69, 102 [antitrust: judges “must give wide berth to business judgments” because they are “neither economic nor industry experts”]; *Gaillard v. Natomas Co.* (1989) 208 Cal.App.3d 1250, 1263 [common law: “those to whom the management of the corporation has been entrusted, and not the courts, are best able to judge whether a particular act or transaction is one which is ‘. . . helpful to the conduct of corporate affairs or expedient for the attainment of corporate purposes” ’’].)

Finally, the difficulty of these inquiries would be compounded by the limited record that courts often have before them when deciding a subpoena dispute. In *Hunter*, this Court could not decide the SCA’s application in the first instance but had to remand for “development of an adequate record.” (*Hunter, supra*, 4 Cal.5th at p. 1251.) In particular, there was “an evidentiary lacuna” on whether the subpoenaed social media posts were from public accounts or private ones. (*Id.* at pp. 1259–1260.) The subpoenas in this case were issued years after *Hunter* was decided, but still “it is not clear from the record . . . whether [Pina’s] Facebook, Instagram, and Snapchat accounts were configured as public or private.” (*Pina, supra*, 103 Cal.App.5th at p. 1061.) Simple historical facts are often murky at the point in litigation when courts are tasked with deciding whether to quash a subpoena.

Yet several versions of the business model theory assume that courts would somehow have the record needed to make complicated findings about computer security and business

necessity. Courts have long been reluctant to weigh in on these subjects, even under the best of procedural conditions. The business model theory would not just task courts with making these long-eschewed decisions but would have courts do so quickly, with limited facts, and often early into litigation. Courts would reach inconsistent results, and questions about the SCA's coverage would spread. Congress could not have wanted such a result when it passed the SCA to ensure businesses' and users' confidence in new communications technologies.

C. Other versions of the business model theory would put courts to a false dilemma of deciding whether a business practice benefits the user or the provider, when in fact it benefits both.

The Court of Appeal, Pina, and the People alternatively suggest versions of the business model theory that would ask courts to determine who is the single party that benefits from a provider's ability to access communications: the user only or the provider only. (See, e.g., *Pina, supra*, 103 Cal.App.5th at pp. 1062–1063 [“own business purposes”]; Pina ABOM 39 [“administrative and safety services that are not for the profit of the company”]; People ABOM 32 [access “on ‘behalf of’ [a provider] [rather than the customer”].) These versions of the business model theory are based on a false dichotomy that ignores the economic reality of online platforms.

Online platforms are often “what economists call a ‘two-sided platform.’” (*Ohio v. American Express Co.* (2018) 585 U.S. 529, 534 [138 S.Ct. 2274, 201 L.Ed.2d 678].) “As the name implies, a two-sided platform offers different products or services

to two different groups who both depend on the platform to intermediate between them.” (*Ibid.*) A defining trait of a two-sided market is the presence of “[i]ndirect network effects,” which means that “the value of the two-sided platform to one group of participants depends on how many members of a different group participate.” (*Id.* at p. 535.)

Social media platforms, for example, bring together two (or more) groups: users and advertisers. (See Crane, *Defining Relevant Markets in Digital Ecosystems* (2024) 7 *Journal of Law & Innovation* 10, 14 [social media platforms “serve and match two populations of users—customers and advertisers—and therefore imply indirect network effects and interdependency of economic effects as competitive conditions change on the two sides of the market”]; Niels & Ralston, *Two-Sided Market Definition: Some Common Misunderstandings* (2021) 17 *European Competition Journal* 118, 119 [“digital platforms” are “often referred to as two-sided platforms as they bring together two (or more) types of user[s]—such as . . . social media sites bringing together users, app developers and advertisers”]; Marchese, *Debunking the “Big Is Bad” Bogeyman* (2020) 28 *Geo. Mason L.Rev.* 1, 15 (hereafter Marchese) [social media platforms “play[] match-maker between users and advertisers, and [they] compete[] for at least two different sets of customers”].)

In a two-sided market, actions that might at first blush seem geared toward only one group also have consequences for the other group. A social media platform may take steps aimed at improving user experience—for example, decreasing the

amount of irrelevant content users see. But if those steps are successful and bring more users to the platform, then they also benefit advertisers by providing them with a larger audience. (See Marchese, *supra*, 28 Geo. Mason L.Rev. at p. 19.) That, in turn, increases the price that the platform is able to charge advertisers and ultimately increases the platform’s revenue. Yet a social media platform might also take steps seemingly aimed at increasing the platform’s value to advertisers—for example, allowing contextual or targeted advertising. If successful, those steps increase the advertising revenue a platform receives. And that revenue, in turn, allows the platform “to remain free for users” and gives the platform the funds needed to “improve[] and innovate[] its products” offered to users. (*Id.* at pp. 19–20.)

Given this economic reality, a platform’s ability to access communications will not generally benefit only the user or only the platform; it will generally benefit *both*. Overlooking this reality, proponents of the business model theory have assumed that two common types of access—screening for illicit content, and facilitating user-tailored advertising—fall on opposite sides of the theory. In their view, screening content benefits only the user, while facilitating advertising benefits only the platform. But as explained below, these two types of access are indistinguishable in terms of who benefits from them. Each benefits both the platform and the user.

Content screening. As the SCA contemplates, online platforms routinely scan communications to detect and report child pornography. (See *ante*, section I.A.; Snap OBOM 57–59 [in

2023, “Snap made over 690,000 reports of suspected child sexual abuse material”).) In a similar vein, virtually all platforms—ranging from messaging applications to search engines to social media platforms to dating sites—implement safety or content-moderation policies under which they remove types of content that they believe would harm their users’ experience.

At least as applied to unlawful content, both the Court of Appeal and Pina treat it as a given that this type of access would not forfeit SCA protection under the business model theory. (*Pina, supra*, 103 Cal.App.5th at pp. 1064–1065 [rejecting argument that the business model theory would “‘negatively impact providers’ ability’ ” to screen and remove “‘illicit content’ ”]; Pina ABOM 38–49 [stating “administrative and safety services” are not barred by the business model theory].) In their view, content screening and moderation benefit only the user—not the platform.

But that assessment is simply not accurate. Removing illegal or otherwise objectionable content undoubtedly benefits users by making them feel safer using, for example, a dating app or social media platform. But as explained, actions that improve user experience attract more users and, in turn, make a platform more valuable to advertisers—benefitting the platform. (Cf. *United States v. Miller* (6th Cir. 2020) 982 F.3d 412, 419.) Neither Pina nor the Court of Appeal explain why their myopic view of who benefits from this type of provider access should prevail over the economic reality that it benefits *both* users and providers.

So while Pina and the Court of Appeal treat this type of access as unaffected by the business model theory, it may well fail the profit-based tests they propose. If so, that would produce a disastrous result: forcing platforms to choose between the SCA's protections and screening illegal or otherwise objectionable content.

Advertising. Many online platforms can offer their services free to users only because the user-side is subsidized by their revenue on the advertiser-side. Indeed, the vast majority of online applications are available to download for free. (See *Epic Games, Inc. v. Apple Inc.* (N.D.Cal. 2020) 493 F.Supp.3d 817, 845 [84 percent of apps on the Apple iOS store are free].) Given consumer preferences, those apps are highly likely to be monetized through contextual or targeted ads rather than a subscription model. (See Interactive Advertising Bureau, *The Free and Open Ad-Supported Internet* (2024) pp. 14–15 <<https://tinyurl.com/447ccf3n>> [as of Feb. 18, 2025] (hereafter IAB Report) [78 percent of users prefer to have free apps supported by ads, and 88 percent of users prefer tailored ads to general ones]; Lebow, *Advertising Makes Up The Lion's Share of Mobile App Revenues* (Sept. 25, 2023) eMarketer <<https://tinyurl.com/2e3x29c3>> [as of Feb. 18, 2025] [from 2020 to 2024, ad revenue constituted about \$160 billion compared to about \$42 billion in content purchases].)

Proponents of the business model theory consider access to facilitate advertising to be an obvious example of when SCA protections would disappear. (*Pina, supra*, 103 Cal.App.5th at

pp. 1053–1054, 1062 & fn. 16, 1063 [describing Meta’s terms of service that allow advertising, and applying the business model theory]; Pina ABOM 5, 38 [“advertising-driven business models exclud[e] companies” from the scope of the SCA]; People ABOM 12 [providers must come “under the SCA at the expense of their advertising revenue”].) In their view, this access benefits only the platform—not the consumer. (See People ABOM 41 [“it is evident” this type of access “is for the purpose of serving Meta’s advertising customers, not their non-paying users”].)

But again, that is simply not true. Allowing data access to facilitate advertising that is more relevant and interesting to each consumer benefits consumers. The vast majority of users—nearly 90 percent—prefer tailored ads to general ones. (IAB Report, *supra*, at p. 15.) A similar percentage of users—87 percent—report that they are more likely to click on a tailored ad than a general one. (*Ibid.*) About 70 percent of users agree that tailored ads help them find products, services, and bargains that interest them. (*Id.* at p. 17.) And again about 70 percent of users report that they are willing to share data about their lifestyle and interests to receive tailored ads. (*Ibid.*) So when an online service provider accesses content to facilitate advertising, it is responding to the majority consumer preference and providing those consumers with a more interesting, engaging experience.

Additionally, advertising revenue is what allows countless technology companies to offer their products to users for free. And advertising revenue is what allows those technology companies to continuously innovate to improve their users’

experience. So in terms of who benefits from the access, advertising-facilitating access is indistinguishable from content-screening access: it benefits *both* consumers and platforms.

Pina, the People, and the Court of Appeal therefore apply the profit-based versions of the business model theory inconsistently—treating two like accesses differently. But even if these versions of the theory were applied in a manner that acknowledged the economic realities governing online platforms and treated like accesses alike, they would run into another problem. Since types of access that benefit users also benefit platforms, a consistent application of these versions of the theory would bar nearly *all* provider access. And as explained, such a no-access-at-all interpretation of the SCA cannot be squared with its text, which assumes provider access. (*Ante*, section I.A.)

III. The business model theory undermines the SCA’s purpose of encouraging businesses’ development and consumers’ use of new communications technologies.

A. The business model theory may mandate that businesses adopt a pay-for-service model.

One of Congress’s purposes in adopting the SCA was to “encourag[e] the use and development of new technologies.” (*Hunter, supra*, 4 Cal.5th at p. 1263; see *O’Grady, supra*, 139 Cal.App.4th at pp. 1444–1445 [“encourage ‘innovative forms’ of communication”].) But the *Touchstone* concurrence candidly admitted that, under the business model theory, providers may need to “revert to an old-school pay-for-service business model” to avoid losing SCA coverage. (*Touchstone, supra*, 10 Cal.5th at p. 372, fn. 14 (conc. opn. of Cantil-Sakauye, C.J.)) Seeking to

encourage innovation, Congress could not have possibly wanted the SCA’s protections to apply only to certain, judicially-prescribed business models.

The status quo allows for “interbrand competition,” producing a “heterogenous market” that is “highly innovative.” (See *Epic Games, supra*, 67 F.4th at pp. 987, 998.) The SCA provides a substantial baseline level of privacy to users for their online communications. In such a heterogenous market, consumers who desire even more privacy above the SCA’s baseline can select providers that forego advertising revenue and instead employ the “pay-for-service” model that is the *Touchstone* concurrence’s preference. By contrast, consumers who most value lower (or no) costs can select providers that are free but facilitate contextual or targeted advertising. (See *ibid.*) The business model theory risks taking that heterogenous market and flattening it—undermining Congress’s intent.

B. The business model theory would unduly burden providers with discovery requests.

The business model theory would also open up providers to discovery requests from private parties, which “would impose severe administrative burdens, interfering with the manifest congressional intent to encourage development and use of digital communications.” (*O’Grady, supra*, 139 Cal.App.4th at p. 1446.)

Responding to routine subpoena requests from private parties would not be a rote task, and opening the floodgates of requests for user communications would be highly burdensome on service providers. The more specific the requests, the more

effort and cost that would be required to search and sort through massive amounts of information. And the broader the requests, the more risk there would be to the privacy interests of users. The costs would not just involve the technological costs of searching, categorizing, compiling, and delivering data. Responses would also require human expertise. For example, service providers would need to analyze data requests, narrowly tailor required responses to the requests, and resist them when appropriate, just as they currently do for government requests. (See Meta, *Government Requests for User Data*, <<https://tinyurl.com/39cjpekr>> [as of Feb. 7, 2025] (hereafter Meta Report) [“Each and every request we receive is carefully reviewed for legal sufficiency and we may reject or require greater specificity on requests that appear overly broad or vague”].)

Responding to the flood of subpoenas allowed by the business model theory would require substantial resources, including in the form of legal fees. (See *O’Grady, supra*, 139 Cal.App.4th at p. 1446 [“Resistance [to routine subpoenas] would likely entail legal expense, and compliance would require devoting some number of person-hours to responding in a lawful and prudent manner”].) Service providers would undoubtedly incur further legal fees from the need to protect themselves against potential civil liability for disclosing information where they were prohibited from doing so, other than in “good faith reliance” on a court order. (See 18 U.S.C. § 2707(a), (e)(1).) It makes little sense to shift the burden of these costs from those

seeking the communications and those privy to the communications to disinterested third-party service providers, “who served only as a medium and neutral repository for the message.” (*O’Grady, supra*, 139 Cal.App.4th at p. 1446.)

Online platforms already expend substantial resources responding to government subpoenas and search warrants allowed under the SCA. Just from January to June 2024, Meta received 323,846 government requests and produced information in response to about 77 percent of them. (Meta Report, *supra*.) If private individuals—whose interests in others’ data can be substantially broader and more disparate than prosecutors and law enforcement—were allowed to seek user communication disclosures from these service providers via subpoena, the floodgates would crash open.

Proponents of the business model theory have failed to grapple with these burdens it would impose. The *Touchstone* concurrence and the Court of Appeal reasoned that the theory would be unlikely to burden providers because “other laws,” such as the Fourth Amendment, “already protect” against disclosure to “law enforcement actors.” (*Touchstone, supra*, 10 Cal.5th at p. 372 (conc. opn. of Cantil-Sakauye, C.J.); *Pina, supra*, 103 Cal.App.5th at p. 1066.) But the protection of the Fourth Amendment is a nonsequitur because the business model theory opens up providers to subpoenas, like those issued here, on behalf of *private* parties who are not bound by constitutional and statutory limits on government action. *Pina* also tries to minimize the consequences of the business model theory by

suggesting it is limited to the criminal context. (See Pina ABOM 10 [“courts have built into the criminal defense subpoena” process certain privacy safeguards], 26, 36, 48 [distinguishing without any explanation “civil cases.”].) But the business model theory (purportedly) interprets the SCA’s disclosure bar. Any holding by this Court would apply to civil and criminal litigants alike.

IV. The business model theory violates the SCA’s purpose of providing stronger privacy protections than the Fourth Amendment.

The business model theory would undermine another purpose of the SCA: “protecting the privacy expectations of citizens.” (*Hunter, supra*, 4 Cal.5th at p. 1263.) As this Court recognized in *Hunter*, Congress passed the SCA against a backdrop of “legal uncertainty” about the government’s ability to access users’ electronic communications. (*Id.* at p. 1263, fn. 16.) Because online communications are “‘subject to control by a third party computer operator,’” Congress worried that the Fourth Amendment’s third-party doctrine might leave online communications “‘subject to no constitutional privacy protection.’” (*Id.* at p. 1263, fn. 15, quoting Sen.Rep. No. 99-541, 2d Sess., p. 3 (1986).)

Congress therefore enacted the SCA to fill that potential gap in the Fourth Amendment’s coverage. The business model theory would produce the anomalous result of making the SCA narrower than the Fourth Amendment—reimposing the very rationale Congress sought to reject and which more recent Fourth Amendment decisions have declined to mechanically extend to

the digital sphere. (See Meta OBOM 9, 29–30; Snap OBOM 16–19, 55–57; Meta RB 16; Snap RB 27.)

The Fourth Amendment’s third-party doctrine is rooted in two Supreme Court decisions: *United States v. Miller* (1976) 425 U.S. 435 [96 S.Ct. 1619, 48 L.Ed.2d 71] (*Miller*) and *Smith v. Maryland* (1979) 442 U.S. 735 [99 S.Ct. 2577, 61 L.Ed.2d 220] (*Smith*). *Miller* held that an individual lacked a reasonable expectation of privacy in “financial statements and deposit slips” shared with his bank because they “contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.” (*Miller*, at p. 442.) *Smith* held that the government’s use of a pen register to track the outgoing phone numbers on a landline telephone did not invade an individual’s privacy because “the phone company [did] in fact record this information for a variety of legitimate business purposes.” (*Smith*, at p. 743.)

The Supreme Court has, however, declined to reflexively extend *Miller* and *Smith* to information shared with online providers. In *Carpenter v. United States*, the Court held that individuals’ reasonable expectation of privacy in their cell-site location information—that is, a record of their physical location based on their cellphone pinging nearby cell-service towers—does not disappear simply because they share that information with their cell-service provider. (*Carpenter v. United States* (2018) 585 U.S. 296, 311 [138 S.Ct. 2206, 201 L.Ed.2d 507] (*Carpenter*) [“Although such records are generated for commercial purposes,

that distinction does not negate [an] anticipation of privacy in his physical location”].)

The Court declined to “mechanically apply[]” *Miller* and *Smith* to “the qualitatively different” and “novel” circumstances before it—noting “the seismic shifts in digital technology” that our society has undergone in recent decades. (*Carpenter, supra*, 585 U.S. at pp. 309, 313–314.) The Court explained that the use of new communications technologies has become a “‘pervasive and insistent part of daily life’” that is unavoidable “[a]part from disconnecting” completely. (*Id.* at p. 315.) So unlike the searches in *Miller* and *Smith* that “reveal[ed] little,” searches of information disclosed to third-party communications technology providers can be highly intrusive—contravening individuals’ expectations of privacy. (*Id.* at p. 314; see *Riley v. California* (2014) 573 U.S. 373, 394 [134 S.Ct. 2473, 189 L.Ed.2d 430] [“Even the most basic phone” can “hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on”].)

In *Carpenter*, the Supreme Court expressly acknowledged that cell-service providers use individuals’ location data “for their own business purposes.” (*Carpenter, supra*, 585 U.S. at p. 301.) But it was of no import to the Court’s decision that those providers access users’ data to “find[] weak spots in their network” and “apply[] ‘roaming’ charges,” or that they “often sell aggregated location records to data brokers.” (*Ibid.*) Individuals still retain a reasonable expectation of privacy.

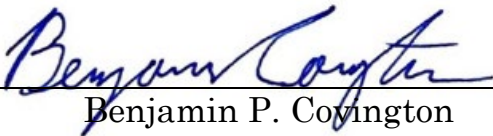
In adopting the business model theory, the Court of Appeal bucked both Congress’s intent to prophylactically account for the third-party doctrine and the Supreme Court’s decision not to mechanically apply that doctrine to the digital sphere. The Court of Appeal categorically concluded that, when “users allow [a provider] to use their content for other purposes, they do not have the expectation of privacy contemplated by the SCA.” (*Pina, supra*, 103 Cal.App.5th at p. 1064; see *id.* at p. 1062 [“the underlying policy purpose of the SCA, to give privacy protections to the users of ECS providers who intend for their communication to be private, is belied where, as here, the users have given the providers authorization to access and use their content for their own purposes”].) A theory of the SCA’s coverage that begins from such a premise simply cannot be a faithful interpretation of the SCA. And such a sweeping (and unsupported) conclusion cannot be squared with the United States Supreme Court’s contrary assessment of individuals’ reasonable expectations of privacy in the modern digital age.

CONCLUSION

For the above reasons, the Court should reject the business model theory and reverse or vacate the judgment of the Court of Appeal.

February 24, 2025

HORVITZ & LEVY LLP
JEREMY B. ROSEN
ERIC S. BOORSTIN
BENJAMIN P. COVINGTON

By: 
Benjamin P. Covington


Attorneys for Amicus Curiae
**CHAMBER OF COMMERCE OF THE
UNITED STATES OF AMERICA**

Document received by the CA Supreme Court.

**CERTIFICATE OF WORD COUNT
(Cal. Rules of Court, rule 8.204(c).)**

The text of this brief consists of 6,245 words as counted by the program used to generate the brief.

Dated: February 24, 2025


Benjamin P. Covington

Document received by the CA Supreme Court.

PROOF OF SERVICE

***Snap, Inc./Meta Platforms Inc. v. The Superior Court of
San Diego County (Pina)***
Case No. S286267

STATE OF CALIFORNIA, COUNTY OF LOS ANGELES

At the time of service, I was over 18 years of age and not a party to this action. I am employed in the County of Los Angeles, State of California. My business address is 3601 West Olive Avenue, 8th Floor, Burbank, CA 91505-4681.

On February 24, 2025, I served true copies of the following document(s) described as **APPLICATION FOR LEAVE TO FILE AMICUS CURIAE BRIEF AND AMICUS CURIAE BRIEF OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA IN SUPPORT OF PETITIONERS SNAP, INC. AND META PLATFORMS INC.** on the interested parties in this action as follows:

SEE ATTACHED SERVICE LIST


BY MAIL: I enclosed the document(s) in a sealed envelope or package addressed to the persons at the addresses listed in the Service List and placed the envelope for collection and mailing, following our ordinary business practices. I am readily familiar with Horvitz & Levy LLP's practice for collecting and processing correspondence for mailing. On the same day that correspondence is placed for collection and mailing, it is deposited in the ordinary course of business with the United States Postal Service, in a sealed envelope with postage fully prepaid.

BY E-MAIL OR ELECTRONIC TRANSMISSION:
Based on a court order or an agreement of the parties to accept service by e-mail or electronic transmission via Court's Electronic Filing System (EFS) operated by ImageSoft TrueFiling (TrueFiling) as indicated on the attached service list:

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

Document received by the CA Supreme Court.

Executed on February 24, 2025, at Sherman Oaks,
California.



Serena L. Steiner

Document received by the CA Supreme Court.

SERVICE LIST
***Snap, Inc./Meta Platforms Inc. v. The Superior Court of
San Diego County (Pina)***
Case No. S286267

INDIVIDUAL / COUNSEL SERVED	PARTY REPRESENTED
L. Ashley Aull (SBN 257020) Munger, Tolles & Olson LLP 350 South Grand Avenue, 50th Floor Los Angeles, CA 90071-3426 (213) 683-9100 ashley.aull@mto.com	Petitioner SNAP, INC. <i>[Via TrueFiling]</i>
J. Max Rosen (SBN 310789) Munger, Tolles & Olson LLP 560 Mission Street, 27th Floor San Francisco, CA 94105-3089 (415) 512-4000 max.rosen@mto.com	Petitioner SNAP, INC. <i>[Via TrueFiling]</i>
David W. Feder (<i>pro hac vice</i>) Fenwick & West LLP 902 Broadway, 18th Floor New York, NY 10010-6035 (212) 430-2600 dfeder@fenwick.com	Petitioner SNAP, INC. <i>[Via TrueFiling]</i>
Tyler G. Newby (SBN 205790) Ryan Kwock (SBN 336414) Fenwick & West LLP 555 California Street, 12th Floor San Francisco, CA 94104-1503 (415) 875-2300 • Fax: (415) 281-1350 tnewby@fenwick.com rkwock@fenwick.com	Petitioner SNAP, INC. <i>[Via TrueFiling]</i>

Document received by the CA Supreme Court.

INDIVIDUAL / COUNSEL SERVED	PARTY REPRESENTED
Janie Y. Miller (SBN 312715) Esther Galan (SBN 335763) Fenwick & West LLP 730 Arizona Avenue, 1st Floor Santa Monica, CA 90401-1702 (310) 434-5400 jmillier@fenwick.com egalan@fenwick.com	Petitioner SNAP, INC. <i>[Via TrueFiling]</i>
Orin S. Kerr (SBN 319808) Law Office of Orin S. Kerr 559 Nathan Abbott Way Stanford Law School Stanford, CA 94305-8602 (650) 498-8125 orin@orinkerr.com	Petitioner SNAP, INC. <i>[Via TrueFiling]</i>
Brian A. Sutherland (SBN 248486) Greg Wolff (SBN 78626) Complex Appellate Litigation Group LLP 96 Jessie Street San Francisco, CA 94105-2923 (415) 649-6700 brian.sutherland@calg.com greg.wolff@calg.com	Petitioner SNAP, INC. <i>[Via TrueFiling]</i>
Julie E. Schwartz (SBN 260624) Ryan T. Mrazik (<i>Pro Hac Vice Requested</i>) John R. Tyler (<i>Pro Hac Vice Requested</i>) Perkins Coie LLP 1201 Third Avenue, Suite 4900 Seattle, WA 98101-3099 (206) 359-8000 • Fax: (206) 359-9000 jschwartz@perkinscoie.com rmrazik@perkinscoie.com rtyler@perkinscoie.com	Petitioner META PLATFORMS INC. <i>[Via TrueFiling]</i>

Document received by the CA Supreme Court.

INDIVIDUAL / COUNSEL SERVED	PARTY REPRESENTED
<p>Natasha Amlani (SBN 322979) Perkins Coie LLP 1888 Century Park East, Suite 1700 Los Angeles, CA 90067-1721 (310) 788-9900 • Fax: (310) 788-3399 namlani@perkinscoie.com</p>	<p>Petitioner META PLATFORMS INC. <i>[Via TrueFiling]</i></p>
<p>Joshua S. Lipshutz (SBN 242557) Gibson, Dunn & Crutcher LLP One Embarcadero Center, Suite 2600 San Francisco, CA 94111-3715 (415) 393-8200 jlipshutz@gibsondunn.com</p>	<p>Petitioner META PLATFORMS INC. <i>[Via TrueFiling]</i></p>
<p>Michael J. Holecek (SBN 281034) Gibson, Dunn & Crutcher LLP 333 South Grand Avenue Los Angeles, CA 90071-3197 (213) 229-7000 • Fax: (213) 229-7520 mholecek@gibsondunn.com</p>	<p>Petitioner META PLATFORMS INC. <i>[Via TrueFiling]</i></p>
<p>Natalie J. Hausknecht (<i>Pro Hac Vice</i>) Gibson Dunn & Crutcher, LLP 1801 California Street, Suite 4200 Denver, CO 80202-2642 (303) 298-5700 nhausknecht@gibsondunn.com</p>	<p>Petitioner META PLATFORMS INC. <i>[Via TrueFiling]</i></p>

Document received by the CA Supreme Court.

INDIVIDUAL / COUNSEL SERVED	PARTY REPRESENTED
<p>Paul A. Rodriguez (SBN 204033) San Diego Public Defender Troy A. Britt (SBN 190879) San Diego Deputy Public Defender Nadine J. Valdecini (SBN 306484) San Diego Deputy Public Defender County of San Diego Office of the Primary Public Defender 451 A Street, Suite 900 San Diego, CA 92101-3624 (619) 338-4700 • Fax: (619) 338-4643 troy.britt@sdcounty.ca.gov nadine.valdecini@sdcounty.ca.gov</p>	<p>Real Party in Interest ADRIAN PINA</p> <p><i>[Via TrueFiling]</i></p>
<p>Summer Stephan (SBN 129323) District Attorney Linh Lam (SBN 241267) Deputy District Attorney Karl Husoe (SBN 261097) Deputy District Attorney Office of San Diego County District Attorney 330 West Broadway, Suite 860 San Diego, CA 92101-3827 (619) 531-4040 • Fax: (619) 237-1351 karl.husoe@sdcca.org</p>	<p>Real Party in Interest THE PEOPLE</p> <p><i>[Via TrueFiling]</i></p>
<p>David L. Jarman (SBN 319896) District Attorney Office of San Diego County District Attorney North County Regional Center 325 South Melrose Drive, Suite 5000 Vista, CA 92081-6691 (760) 806-4004 • Fax: (760) 806-4162 david.jarman@sdcca.org</p>	<p>Real Party in Interest THE PEOPLE</p> <p><i>[Via TrueFiling]</i></p>

Document received by the CA Supreme Court.

INDIVIDUAL / COUNSEL SERVED	PARTY REPRESENTED
California Court of Appeal Fourth District, Division One Symphony Towers 750 B Street, Suite 300 San Diego, CA 92101 (619) 744-0760	Case Nos. D083446/D083475 <i>[Via TrueFiling]</i>
Clerk, San Diego County Superior Court c/o Hon. Daniel F. Link, Dept. NC-21 North County Regional Center 325 South Melrose Drive Vista, CA 92081 (760) 201-8021	Respondent Trial Court Judge Case No. CN429787 <i>[Via U.S. Mail]</i>

Document received by the CA Supreme Court.