

S245203

COPY

SUPREME COURT
FILED

MAY 17 2018

Jorge Navarrete Clerk

IN THE
SUPREME COURT OF CALIFORNIA

Deputy

CRC
8.25(b)

FACEBOOK, INC.,
Petitioner,

v.

**SUPERIOR COURT OF CALIFORNIA FOR
THE COUNTY OF SAN DIEGO,**
Respondent,

LANCE TOUCHSTONE,
Real Party in Interest.

AFTER A DECISION BY THE COURT OF APPEAL, FOURTH APPELLATE DISTRICT, DIVISION ONE
CASE No. D072171

**APPLICATION TO FILE AMICI CURIAE BRIEF;
AMICI BRIEF OF APPLE INC., GOOGLE INC.,
OATH INC., TWITTER, INC., AND CALIFORNIA
CHAMBER OF COMMERCE IN SUPPORT OF
PETITIONER FACEBOOK, INC.**

HORVITZ & LEVY LLP
JEREMY B. ROSEN (BAR No. 192473)
*STANLEY H. CHEN (BAR No. 302429)
3601 WEST OLIVE AVENUE, 8TH FLOOR
BURBANK, CALIFORNIA 91505-4681
(818) 995-0800 • FAX: (844) 497-6592
jrosen@horvitzlevy.com
schen@horvitzlevy.com

ATTORNEYS FOR AMICI CURIAE
**APPLE INC., GOOGLE INC., OATH INC., TWITTER, INC., AND
CALIFORNIA CHAMBER OF COMMERCE**

TABLE OF CONTENTS

| | Page |
|---|-------------|
| TABLE OF AUTHORITIES | 4 |
| APPLICATION TO FILE AMICI CURIAE BRIEF | 10 |
| AMICI CURIAE BRIEF..... | 14 |
| INTRODUCTION..... | 14 |
| LEGAL ARGUMENT..... | 15 |
| I. The Stored Communication Act’s prohibition against disclosure of communications is purposefully broad, with its exceptions narrowly tailored. | 15 |
| A. The text and structure of the SCA calls for a broad prohibition against disclosure of electronic communications..... | 15 |
| B. The broad prohibition against disclosure comports with the purposes of the SCA..... | 19 |
| II. Carving out court-created exceptions to the SCA’s prohibition on disclosure would erode users’ privacy interests. | 22 |
| A. The SCA’s prohibition on disclosure is necessary to protect users’ privacy interests in modern communications..... | 22 |
| B. Opening up disclosure of communications to private individuals would erode users’ privacy interests. | 26 |
| III. Allowing direct disclosure would undermine user confidence in technology and hinder its development. | 28 |
| IV. Allowing direct disclosure of user communications would be unduly burdensome on providers. | 32 |
| CONCLUSION..... | 36 |

CERTIFICATE OF WORD COUNT 37

TABLE OF AUTHORITIES

| | Page(s) |
|--|------------|
| Cases | |
| <i>Chevron U.S.A. Inc. v. Echazabal</i> (2002) 536 U.S. 73 [122 S.Ct. 2045, 153 L.Ed.2d 82]..... | 17 |
| <i>Howard Jarvis Taxpayers Assn. v. Padilla</i> (2016) 62 Cal.4th 486..... | 17 |
| <i>In re Malik J.</i> (2015) 240 Cal.App.4th 896 | 25 |
| <i>In re Ricardo P.</i> (2015) 241 Cal.App.4th 676, review granted Feb. 17, 2016, S230923 | 25 |
| <i>Krinsky v. Doe 6</i> (2008) 159 Cal.App.4th 1154 | 31 |
| <i>Mintz v. Mark Bartelstein & Associates, Inc.</i> (C.D.Cal. 2012) 885 F.Supp.2d 987..... | 19 |
| <i>O’Grady v. Superior Court</i> (2006) 139 Cal.App.4th 1423 | passim |
| <i>Packingham v. North Carolina</i> (2017) 582 U.S. ____ [137 S.Ct. 1730, 198 L.Ed.2d 273]..... | 24 |
| <i>Riley v. California</i> (2014) 573 U.S. ____ [134 S.Ct. 2473, 189 L.Ed.2d 430]..... | 24, 25, 26 |
| <i>Theofel v. Farey-Jones</i> (9th Cir. 2004) 359 F.3d 1066..... | 21 |
| <i>United States v. Erika, Inc.</i> (1982) 456 U.S. 201 [102 S.Ct. 1650, 72 L.Ed.2d 12]..... | 18 |

| | |
|---|--------|
| <i>United States v. Jones</i> (2012) 565 U.S. 400 [132 S.Ct. 945, 181 L.Ed.2d 911]..... | 26, 27 |
| <i>United States v. LaCoste</i> (9th Cir. 2016) 821 F.3d 1187..... | 23 |

Statutes

| | |
|--------------------------|--------------------|
| 12 U.S.C. § 3403(a)..... | 18 |
| 18 U.S.C. | |
| § 2701 | 16, 17 |
| § 2701(a) | 17 |
| § 2702 | 15, 16, 17, 18, 21 |
| § 2702(a) | 14 |
| § 2702(a)(1) | 16 |
| § 2702(a)(2) | 16 |
| § 2702(b)(1) | 17 |
| § 2702(b)(1)-(9) | 16 |
| § 2702(3) | 17 |
| § 2703 | 16, 17, 18, 28 |
| § 2703(b)(1)(B) | 28 |
| § 2704 | 18 |
| § 2705 | 18 |
| § 2706 | 18 |
| § 2706(a) | 35 |
| § 2707(a) | 18, 34 |
| § 2707(e)(1) | 34 |
| Penal Code, § 1326 | 28 |

Rules of Court

| | |
|------------------------|----|
| Cal. Rules of Court | |
| rule 8.200(c)(3)..... | 11 |
| rule 8.520(f)(1) | 10 |

Miscellaneous

| | |
|---|----------------|
| Apple, <i>Report on Government and Private Party Requests for Customer Information: January 1-June 30, 2017</i> < https://apple.co/2xO5fLM > | 33, 35 |
| Bahl, Cognizent, <i>The Business Value of Trust</i> (May 2016) < https://cogniz.at/2oSvv4y >..... | 31 |
| Booton, <i>Fitbit Aims to Track Women’s Health and Kids’ Activity</i> , SportTechie (Mar. 13, 2018) < https://bit.ly/2jI7MyX >..... | 25 |
| Dropbox, <i>Transparency Reports</i> < https://bit.ly/2KMLXdH >..... | 35 |
| Facebook, <i>Information for Law Enforcement Authorities</i> < https://bit.ly/2G0Uzty >..... | 32 |
| Facebook, <i>Transparency Report for the United States: Law Enforcement Requests for Data</i> < https://bit.ly/2jM2TVz >..... | 35 |
| Goldberg, National Telecommunications and Information Administration, <i>Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities</i> (May 13, 2016) < https://bit.ly/27jJfSX > | 30 |
| Google, <i>Transparency Report for United States: Requests for User Information</i> < https://bit.ly/2KaALXp >..... | 35 |
| H.R.Rep. No. 99-647, 2d Sess. (1986)..... | 19, 20, 21, 28 |
| Hearing before Sen. Com. on Judiciary, Subcom. on Patents, Copyrights and Trademarks, on Sen. No. 1667, 99th Cong., 1st Sess. (1985)..... | 20 |
| Hearings before House Com. on Judiciary, Subcom. of Courts, Civil Liberties, and the Administration of Justice, 99th Cong., 1st and 2d Sess. (1986) | 29 |

| | |
|--|--------|
| Hill, <i>This Sex Toy Tells the Manufacturer Every Time You Use It</i> , Fusion (Aug. 9, 2016) < https://bit.ly/2I6A68I > | 26 |
| Horrigan, Pew Research Center, <i>Use of Cloud Computing Applications and Services</i> (2008)..... | 23 |
| Internet Policy Task Force, Department of Commerce, <i>Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework</i> (Dec. 16, 2010) < https://bit.ly/2K80Oyt > | 30 |
| Mobile Fact Sheet, Pew Research Center (2017) | 23 |
| Moynihan, <i>Alexa and Google Home Record What You Say. But What Happens to that Data?</i> , Wired (Dec. 5, 2016) < https://bit.ly/2gY9qKG >..... | 26 |
| Note, <i>Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act</i> (2010) 98 Geo. L.J. 1195 | 26 |
| Note, <i>Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment</i> (2009) 78 Fordham L.Rev. 349 | 22, 24 |
| Oath, <i>Transparency Report for the United States: Law Enforcement Data Requests</i> < https://bit.ly/2jKGZ54 > | 35 |
| Off. of Technology Assessment, U.S. Cong., <i>Federal Government Information Technology: Electronic Surveillance and Civil Liberties</i> (1985) | 20, 29 |
| Pub.L. No. 99-508 (Oct. 21, 1986) 100 Stat. 1860 | 16 |
| Rainie, Pew Research Center, <i>The State of Privacy in Post-Snowden America</i> (2016)..... | 24, 25 |

| | |
|---|---------------|
| Remarks of Sen. Leahy, 132 Cong. Rec. 7992 (1986)..... | 29 |
| Sen.Rep. No. 99-541, 2d Sess. (1986)..... | <i>passim</i> |
| Simon, <i>With New EKG Monitor and Heart Study App, Apple Watch Could One Day Save Your Life</i> , Macworld (Nov. 30, 2017) < https://bit.ly/2wp3NQU > | 25 |
| Smith, Pew Research Center, U.S. Smartphone Use in 2015 (2015)..... | 23 |
| Smith & Anderson, Pew Research Center, Online Shopping and E-Commerce (2016)..... | 23 |
| Smith & Anderson, Pew Research Center, Social Media Use in 2018 (2018) | 23 |
| Stewart, <i>Applying for Food Stamps in New York? There's an App for That</i> , N.Y. Times (July 24, 2017)..... | 24 |
| The Radicati Group Inc., Email Statistic Report, 2017-2021: Executive Summary (2017) | 23 |
| Twitter, <i>Guidelines for Law Enforcement</i> < https://bit.ly/2IbM00W >..... | 32 |
| Twitter, <i>Transparency Report for United States: Information Requests January to June 2017</i> < https://bit.ly/2K9OLAt > | 35 |
| United States Securities and Exchange Commission, Facebook First Quarter 2018 Form 10-Q < https://bit.ly/2K8GrRs > | 32 |
| USCIS Website, <i>E-Verify Now Optimized for Mobile Devices</i> < https://bit.ly/2FYvH5E > | 23 |
| Weigel, <i>'Fitbit for Your Period': The Rise of Fertility Tracking</i> , Guardian (Mar. 23, 2016) < https://bit.ly/2jPPl9r > | 26 |

Wikipedia, List of Virtual Communities with More
than 100 Million Active Users
<<https://bit.ly/1RuUNJA>>..... 23

IN THE
SUPREME COURT OF CALIFORNIA

FACEBOOK, INC.,
Petitioner,

v.

SUPERIOR COURT OF CALIFORNIA FOR
THE COUNTY OF SAN DIEGO,
Respondent,

LANCE TOUCHSTONE,
Real Party in Interest.

APPLICATION TO FILE AMICI CURIAE
BRIEF

Pursuant to California Rules of Court, rule 8.520(f)(1), amici Apple Inc., Google Inc., Oath Inc., Twitter, Inc., and the California Chamber of Commerce request permission to file the attached amici curiae brief in support of petitioner Facebook, Inc.¹

Amici represent the interests of some of the world's leading technology companies. Billions of people rely daily on these companies' search engines, email services, social networks,

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 amici, their members, or their counsel made a monetary contribution intended to fund the preparation or submission of the proposed brief. (See Cal. Rules of Court, rule 8.200(c)(3).)

communication platforms, smartphones, cloud storage, and Internet-based devices and applications. Users entrust these companies with some of their most important information. Given the sensitivity of this data, these companies work continuously to secure their users' privacy.

Amici's interest in this case arises out of concern for the important privacy interests of the individuals that use online services, the impact on technology companies of the high cost and burden of responding to routine subpoenas from third parties, and the potential civil liability involved in acting contrary to federal law.

Apple Inc. (Apple) offers highly secure hardware, software, and servers to customers worldwide. Apple's business strategy leverages its unique ability to design and develop its own operating systems, hardware, application software, and services to provide customers products and solutions with superior security, ease of use, seamless integration, and innovative design. In addition to the iPhone, iPad, Mac computer, and iPod, Apple offers its users iCloud—a cloud service for storing photos, contacts, calendars, documents, device backups, and more, keeping everything up to date and available to customers on whatever device they are using. Apple is committed its users' privacy and to helping users understand how it handles their personal information.

Google Inc. (Google) is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of web-based products and services, including Search, Gmail, Maps, YouTube, and Blogger, that are used daily around the world. For

example, more than 400 hours of YouTube videos are uploaded to Google every minute, and there are more than a billion monthly active users of Gmail. To use these and other services, users give Google information, including queries for Search, photographs for Photos, documents in Drive, emails in Gmail, and videos for YouTube. Google's Privacy Policy helps users understand what data Google collects, why it's collected, and what Google does with it. Google also regularly publishes transparency reports that reflect the volume and type of requests for disclosure of user data that Google receives from government entities.

Oath Inc. (Oath), a Verizon subsidiary, is a values-led company committed to building brands people love, including communications products that include Yahoo Mail and AOL Mail. Oath reaches one billion people around the world with a dynamic house of media and technology brands. Oath publishes information twice a year in transparency reports to provide insight into the requests it receives from governments for information about its users and how it responds to these requests.

Twitter, Inc. (Twitter) is a technology company based in San Francisco, California. Its primary service, Twitter, is a global platform for public self-expression and conversation in real time. Twitter allows people to consume, create, distribute, and discover content and has democratized content creation and distribution. Twitter has more than 300 million monthly active users, spanning nearly every country, and creating approximately 500 million Tweets every day. One of Twitter's core values is defending users' freedom of expression and privacy. Twitter carefully reviews

requests for user information and releases regular transparency reports detailing government requests for user data.

The California Chamber of Commerce (CalChamber) is a non-profit business association with over 13,000 members, both individual and corporate, representing virtually every economic interest in California. For over 100 years, CalChamber has been the voice of California business. While CalChamber represents several of the largest corporations in California, seventy-five percent of its members have 100 or fewer employees. CalChamber acts on behalf of the business community to improve the state's economic and jobs climate by representing businesses on a broad range of legislative, regulatory, and legal issues. CalChamber often advocates before the courts by filing amicus curiae briefs in cases involving issues of paramount concern to the business community, and it counts among its members many technology companies who are concerned about their users' privacy interests.

May 11, 2018

HORVITZ & LEVY LLP
JEREMY B. ROSEN
STANLEY H. CHEN

By: _____



Stanley H. Chen

Attorneys for Amici Curiae
**APPLE INC., GOOGLE INC., OATH
INC., TWITTER, INC., AND
CALIFORNIA CHAMBER OF
COMMERCE**

AMICI CURIAE BRIEF

INTRODUCTION

On its face, the Stored Communications Act (SCA) plainly prohibits service providers such as Facebook and amici from disclosing their users' private communications. (See 18 U.S.C. § 2702(a).)² Despite this, real party in interest Lance Touchstone wants this prohibition to be invalidated because “[t]echnology has changed,” and “[t]here are more efficient methods of conveying information and transmitting data.” (RBOM 9.) With such technology changes, he argues, there should be no need to hold him to “antiquated standards of production” of the communications of third party individuals because the technological changes supposedly come with “drawbacks,” such as decreased privacy rights. (*Ibid.*) Touchstone is wrong, and this Court should not deviate from the plain text and purpose of the SCA.

Even in 1986 when the SCA was enacted, Congress was aware of the possibility that there would be an increased demand for individuals' private communications as they became electronic, concomitant with an increased ease of access to those communications. Indeed, these ominous possibilities are why Congress enacted the SCA—to protect privacy and encourage technology to flourish. And flourish it has—today, technology companies serve billions of people who are not expecting their

² All further statutory references are to title 18 of the United States Code unless otherwise indicated.

private communications to be released as Touchstone proposes here, no matter how fast a computer can copy and send data.

Touchstone's basis for trying to ride roughshod over the clear prohibitions in the SCA is that doing so is the only way to preserve his constitutional rights. Amici agree with petitioner Facebook that Touchstone's constitutional arguments have no merit. With this brief, amici seek to further explain just how heavily Touchstone's lax attitude towards established user privacy protections cuts against the important interests that Congress was attempting to protect in enacting the SCA.

LEGAL ARGUMENT

- I. The Stored Communication Act's prohibition against disclosure of communications is purposefully broad, with its exceptions narrowly tailored.**
- A. The text and structure of the SCA calls for a broad prohibition against disclosure of electronic communications.**

The text and structure of the SCA make it clear that its broad prohibition on the disclosure of user communications by electronic service providers (§ 2702) contains no exception for responding to subpoenas from nongovernmental parties. They also make it clear that such broad protection was purposeful.

In 1986, Congress enacted the SCA as a part of the Electronic Communications Privacy Act (ECPA), which amended the federal wiretap law. (Pub.L. No. 99-508 (Oct. 21, 1986) 100 Stat. 1860.) The ECPA consists of three major parts: Title I governs the interception of wire, oral, and electronic communications; title II, the SCA, governs access to stored electronic communications and records; and title III governs pen registers and trap and trace devices. (See Sen.Rep. No. 99-541, 2d Sess., p. 3 (1986) (hereafter Sen.Rep.)) The SCA itself contains a number of key provisions. The first makes unauthorized access to electronic communications a criminal offense. (See § 2701.) The second governs voluntary disclosure of communications, prohibiting service providers from divulging communications except under limited circumstances. (See § 2702.) The third governs required disclosure of communications, establishing a multi-tiered framework by which government actors can seek communications from providers if they have legitimate law enforcement purposes and undergo certain legal processes. (See § 2703.)

Section 2702 of the statute expressly provides that a service provider “shall not knowingly divulge to *any person or entity* the contents of any communications” it is storing or carrying. (§ 2702 (a)(1), emphasis added; see also § 2702(a)(2).) The same section comprehensively lists nine specific exceptions to the prohibition, but none of them include private individuals seeking discovery. (§ 2702(b)(1)-(9).) As one Court of Appeal has remarked in a similar context, there are “[f]ew cases [that] provide[] a more appropriate occasion to apply the maxim *expressio unius exclusio alterius est.*”

(*O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 1443 (*O'Grady*) [applying maxim to hold that section 2702's prohibition on disclosure has no exception for responding to civil discovery subpoenas]; see also *Howard Jarvis Taxpayers Assn. v. Padilla* (2016) 62 Cal.4th 486, 514 [text of a statute is indicative of intentional design to exclude where it "contain[s] a specific list or facially comprehensive treatment"].)³

The overall structure of the SCA further supports the understanding that section 2702 does not contain an implicit exemption from its prohibition for disclosures to private individuals. On its face, the statute does not just deal with government actors, but comprehensively addresses both private and government actors. For instance, while section 2703 deals with how law enforcement can gain access to information, section 2701 prevents *any* unauthorized persons from accessing such communications without authority. (See § 2701(a) [making it an offense to "intentionally access[] without authorization a facility through which an electronic communication service is provided"].)

In addition, where the statute does provide specific avenues by which law enforcement can access electronic communications, it

³ Notably, the list of exceptions does not just include ones that depend on the actions or identity of government actors or service providers, but also includes several that depend on the actions or identity of *private individuals*. (See § 2702(b)(1), (3); *Chevron U.S.A. Inc. v. Echazabal* (2002) 536 U.S. 73, 81 [122 S.Ct. 2045, 153 L.Ed.2d 82] [expressio unius applies where there is a series that "should be understood to go hand in hand, which is abridged in circumstances supporting a sensible inference that the term left out must have been meant to be excluded"].)

does not do so by providing a simple, unlimited exception for any government actors who seek the information. On the contrary, it provides a *detailed* framework, with varying procedures for varying types of information (see § 2703), varying avenues by which users must be given notice (see §§ 2703-2705), and even criteria for when costs incurred by the provider must be reimbursed (see § 2706). That there is no similar, detailed framework for allowing disclosures to private individuals underscores the purposefulness of the broad prohibition against any such disclosure. (See *United States v. Erika, Inc.* (1982) 456 U.S. 201, 208 [102 S.Ct. 1650, 72 L.Ed.2d 12] [“in the context of [a] statute’s precisely drawn provisions, [an] omission provides persuasive evidence that Congress deliberately intended to foreclose [the omission]”).)⁴

Finally, the statute also gives teeth to the broad disclosure prohibition in section 2702 by providing a civil remedy that is broad enough to allow a user to bring a cause of action against a service provider that improperly disclosed his or her communications. (See § 2707(a).)

⁴ Similarly, Congress clearly could have limited title 18 of the United States Code section 2702 to prohibiting disclosure to the government, much like the Right to Financial Privacy Act that it was generally modeled after. (See Sen.Rep., *supra*, at p. 3 [noting that the SCA is “modeled after the Right to Financial Privacy Act”]; 12 U.S.C. § 3403(a) [Right to Financial Privacy Act expressly prohibiting financial institution from providing financial information “to any Government authority”].) But just as clearly, it did not. (18 U.S.C. § 2702.)

B. The broad prohibition against disclosure comports with the purposes of the SCA.

While the SCA broadly prohibits service providers from disclosing user communications, criminal defendants such as Touchstone are left with the avenues of production aptly described by Facebook in its answering brief on the merits—avenues that largely involve compelling those persons who are *actually privy* to the communications to produce them. (ABOM 18-37.) As several courts interpreting the SCA have acknowledged, “it would be far from irrational for Congress to conclude that one seeking disclosure of the contents of e-mail, like one seeking old-fashioned written correspondence, should direct his or her effort to the parties to the communication and not to a third party who served only as a medium and neutral repository for the message.” (*O’Grady, supra*, 139 Cal.App.4th at p. 1446; accord, *Mintz v. Mark Bartelstein & Associates, Inc.* (C.D.Cal. 2012) 885 F.Supp.2d 987, 994.) Indeed, as we now explain, not only is it far from irrational, it fits hand in glove with the purposes of the SCA as illuminated by the legislative history.

The possibility of a revamped federal wiretap law was brought to Congress’s attention at a time when Congress was worried about several things. First, new technologies were increasing the risk that private communications would be accessed wrongfully “by law enforcement authorities *as well as* unauthorized private parties.” (Sen.Rep., *supra*, at p. 3, emphasis added; see also *id.* at p. 5; H.R.Rep. No. 99-647, 2d Sess., p. 18 (1986) (hereafter H.R.Rep.).)

Second, statutory protections were necessary to balance the interests of law enforcement and users' privacy interests, as well as "ensure the continued vitality of the Fourth Amendment." (H.R.Rep., *supra*, at p. 19; see also Sen.Rep., *supra*, at pp. 3, 5.)

The same concerns are reflected in a report prepared by the Office of Technology Assessment (OTA) at the request of the House Committee on the Judiciary. (See Off. of Technology Assessment, U.S. Cong., Federal Government Information Technology: Electronic Surveillance and Civil Liberties (1985) pp. iii, 48 (hereafter Federal Government Information Technology) ["The contents of electronic mail communications are of interest to the same parties that are interested in the contents of first-class mail communications. Thus, Government officials might be interested in . . . [them]. Private parties might be interested in . . . [them]."]) Indeed, even the American Civil Liberties Union's statements during House and Senate subcommittee hearings leading up to the passage of the statute remarked on *both* of these purposes, not just on concerns about government access and the Fourth Amendment. (See, e.g., Hearing before Sen. Com. on Judiciary, Subcom. on Patents, Copyrights and Trademarks, on Sen. No. 1667, 99th Cong., 1st Sess., p. 132 (1985), written testimony of Jerry J. Berman on behalf of The American Civil Liberties Union [ECPA would protect communications "held by providers of electronic communications services such as electronic mail companies by making it a crime for any person to gain unauthorized access and obtain or alter such records and by making service providers subject to civil liability if they divulge such records. The government must obtain a title III

warrant or court order based on reasonable suspicion to search and seize such records.”])

In other words, it was clear that in passing the SCA, Congress was focused *broadly* on protecting the privacy interests of users of electronic services against both private and government access. This broad purpose is directly reflected in the “general prohibitions on the disclosure of contents” in section 2702. (H.R.Rep., *supra*, at p. 64; see also *id.* at p. 72.) As the Senate Report put it, section 2702 “generally prohibits the provider of a[n] . . . [electronic] service to the public from knowingly divulging the contents of any communication . . . to any person other than the addressee or intended recipient.” (Sen.Rep., *supra*, at p. 37, emphasis added.) The SCA thus “reflects Congress’s judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, [citation], the Act protects users whose electronic communications are in electronic storage.” (*Theofel v. Farey-Jones* (9th Cir. 2004) 359 F.3d 1066, 1072-1073.)

II. Carving out court-created exceptions to the SCA’s prohibition on disclosure would erode users’ privacy interests.

A. The SCA’s prohibition on disclosure is necessary to protect users’ privacy interests in modern communications.

Even in 1986, Congress was concerned with the fact that the rapid speed at which technology develops would outpace the law, and enacted the SCA to legislate broadly in order to protect privacy in the face of ongoing technological change. (See Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment* (2009) 78 Fordham L.Rev. 349, 374 (hereafter *Protections for Electronic Communications*) [noting Senator Patrick Leahy’s remark in a subcommittee hearing about the ECPA: “ ‘rules [concerning privacy] don’t change at all. The technology changes. All the legislation does is to make sure that that the rules stay consistent with the technology’ ”]; see *ibid.* [Representative Robert Kastenmeier’s remark in introducing the bill to the House: “ ‘[a]ny attempt to write a law which tries to protect only those technologies which exist in the marketplace today . . . is destined to be outmoded within a few years’ ”].)

Electronic communications now take place using Internet technology that did not exist in 1986 and has grown to become part of everyday life. Email, social media, web-based communication

services and platforms, and Internet-enabled mobile devices are all ubiquitous.⁵

This expanding technology is far from merely a convenience. People use it for emergencies and safety.⁶ They use it during and for work, as well as to “find[] and apply[] for work.” (*United States v. LaCoste* (9th Cir. 2016) 821 F.3d 1187, 1191.) They use it to participate in economic life.⁷ They even use it to access government services.⁸ Finally, social media and online communications

⁵ Two hundred and sixty-nine billion emails are sent and received daily worldwide. (See The Radicati Group Inc., *Email Statistic Report, 2017-2021: Executive Summary* (2017) p. 2.) Two-thirds of adult Americans are on Facebook, many millions of active users are on Google+, Instagram, LinkedIn, Snapchat, and Twitter, and a majority of Internet users use web-based applications. (See Smith & Anderson, *Pew Research Center, Social Media Use in 2018* (2018) pp. 2-3 [68 percent of American adults use Facebook, 78 percent of 18- to 24-year-olds use Snapchat, three-quarters of Facebook users visit the site daily, and the median American uses three of eight social media platforms]; Horrigan, *Pew Research Center, Use of Cloud Computing Applications and Services* (2008) p.1 [69 percent of internet users have either stored data online or used web-based applications]; see also Wikipedia, *List of Virtual Communities with More than 100 Million Active Users* <<https://bit.ly/1RuUNJA>> [listing, in the United States, e.g., Facebook, Twitter, and Google].) And a vast majority of Americans use mobile devices. (See *Mobile Fact Sheet*, *Pew Research Center* (2017).)

⁶ See Smith, *Pew Research Center, U.S. Smartphone Use in 2015* (2015) (“Fully 53% of smartphone owners indicate that they have been in an emergency situation where having their phone available helped resolve the situation”).

⁷ See Smith & Anderson, *Pew Research Center, Online Shopping and E-Commerce* (2016).

⁸ Indeed, the government sometimes promotes the use of online services. (See, e.g., *USCIS Website, E-Verify Now Optimized for* (continued...))

platforms can be used to engage in First Amendment activity, such as sharing news and political views, associating with others, and organizing public events. (See, e.g., *Packingham v. North Carolina* (2017) 582 U.S. ___, ___ [137 S.Ct. 1730, 1735-1736, 198 L.Ed.2d 273] “[S]ocial media users employ these websites to engage in a wide array of protected First Amendment activity on topics ‘as diverse as human thought’ ”.)

All these Internet-enabled electronic communications typically rely on service providers such as Facebook, transiting through and stored in their facilities. (See *Riley v. California* (2014) 573 U.S. ___, ___ [134 S.Ct. 2473, 2491, 189 L.Ed.2d 430] (*Riley*) [data stored on the “cloud” with “increasing frequency”]; *Protections for Electronic Communications, supra*, 78 Fordham L.Rev. at pp. 378-379 [email routinely held on provider servers for increasing periods of time, and third parties increasingly used for remote storage].)

Given these technological changes, users need to be able to have appropriate control of their personal data and make informed choices about the privacy of their communications. Nearly three-fourths of Americans say that it is “‘very important’ ” to be “in control of who can get information about them,” and a clear majority say it is “‘very important’ ” to be able to control “what information is collected about them.” (Rainie, Pew Research Center, *The State*

(...continued)

Mobile Devices <<https://bit.ly/2FYvH5E>> [as of May 10, 2018]; Stewart, *Applying for Food Stamps in New York? There’s an App for That*, N.Y. Times (July 24, 2017.)

of Privacy in Post-Snowden America (2016).) This desire for control makes sense, given that many users consider their online communications nearly as sensitive as information about health (*ibid.*)—indeed, with “smart” wearable technologies, a user can choose to make health information part of their online data. (See, e.g., Booton, *Fitbit Aims to Track Women’s Health and Kids’ Activity*, SportTechie (Mar. 13, 2018) <<https://bit.ly/2jI7MyX>> [as of May 10, 2018]; Simon, *With New EKG Monitor and Heart Study App, Apple Watch Could One Day Save Your Life*, Macworld (Nov. 30, 2017) <<https://bit.ly/2wp3NQU>> [as of May 10, 2018].)

Courts have also acknowledged the importance of protecting user privacy in the face of rapid technological change. For instance, the United States Supreme Court has made it clear in the Fourth Amendment context that “[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life.’ ” (*Riley*, *supra*, 134 S.Ct. at pp. 2494-2495; see also *In re Malik J.* (2015) 240 Cal.App.4th 896, 900, 902 [probation condition requiring juvenile turn over passwords to social media sites and unfettered search access to his electronic devices may “significantly encroach[] on his and potentially third parties’ constitutional rights of privacy and free speech”].⁹) This is due in part to the storage capacities of modern devices (*Riley*, at p. 2489); the “pervasiveness” of cell phones in the digital age (*id.* at p. 2490 [“it is no exaggeration to say that

⁹ The issue of the constitutionality of such probation conditions is currently being reviewed by this Court. (See *In re Ricardo P.* (2015) 241 Cal.App.4th 676, review granted Feb. 17, 2016, S230923.)

many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate”]); and the methods by which our electronic devices interact with the Internet (*id.* at p. 2491). (See also *United States v. Jones* (2012) 565 U.S. 400, 429 [132 S.Ct. 945, 181 L.Ed.2d 911] (*Jones*) (conc. opn. of Sotomayor, J.) [“The availability and use of these and other new devices will continue to shape the average person’s expectations about the privacy of his or her daily movements”].)

B. Opening up disclosure of communications to private individuals would erode users’ privacy interests.

Congress intended for the SCA to establish durable privacy protections as communications technology grew advanced, even for things unforeseen in 1986 like Web-based email, “cloud” computing, and the “Internet of Things.”¹⁰ Yet Touchstone attempts to turn this intent on its head, arguing that technology growth and innovation should be reason to ignore the SCA. He contends that

¹⁰ See, e.g., Weigel, ‘Fitbit for Your Period’: The Rise of Fertility Tracking, *Guardian* (Mar. 23, 2016) <<https://bit.ly/2jPP19r>> (as of May 10, 2018); Hill, *This Sex Toy Tells the Manufacturer Every Time You Use It*, *Fusion* (Aug. 9, 2016) <<https://bit.ly/2I6A68I>> (as of May 10, 2018); Moynihan, *Alexa and Google Home Record What You Say. But What Happens to that Data?*, *Wired* (Dec. 5, 2016) <<https://bit.ly/2gY9qKG>> (as of May 10, 2018); see also Note, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act* (2010) 98 *Geo. L.J.* 1195, 1223 (questioning whether the SCA would cover newer cloud computing services).

modern “methods of conveying information and transmitting data” are vastly “more efficient,” and dramatically highlights the pervasiveness of Facebook’s role in modern communications. (RBOM 8-9.) As explained above, the implication that Congress wanted to draw in 1986 from the fact that technology rapidly changes was clear: through the SCA, our privacy interests in modern communications are as protected as our traditional communications were, no matter the exact technological methods of their storage or delivery. But that is not the implication Touchstone wants to draw. Instead, Touchstone argues that our privacy rights have “change[d]” as a result of this rapid technology change, and that this should make it *easier* for him to access other peoples’ communications. (RBOM 9.) If it were otherwise, he claims, criminal process would amount to litigation “via carrier pigeon.” (*Ibid.*)

However, in suggesting that privacy rights have changed because the digital era effectively requires our communications to be routed through third parties, Touchstone is incorrectly “treat[ing] secrecy as a prerequisite for privacy.” (*Jones, supra*, 565 U.S. at p. 418 (conc. opn. of Sotomayor, J.) [suggesting that merely voluntarily disclosing some information for a limited purpose does not mean one’s privacy interest in it disappears].) The entire point of the SCA was to maintain privacy rights even as technology expanded and changed—that is, to maintain our privacy rights *as if carrier pigeons were still around*. (See *O’Grady, supra*, 139 Cal.App.4th at p. 1446.)

Touchstone pays short shrift to legislative policy decisions and users' privacy interests, suggesting only that this Court can engraft an exception onto the SCA's prohibition on disclosure using the SCA's subpoena procedures in title 18 of the United States Code section 2703 or the subpoena procedures in Penal Code section 1326. (OBOM 36.) Touchstone claims these procedures—which do not involve the parties actually privy to the requested communications—are sufficient to protect users' privacy interests, but as explained above, Congress clearly disagreed.¹¹ This Court should not interfere with congressional judgment and policy-making to water down the SCA's intended, and important, privacy protections.

III. Allowing direct disclosure would undermine user confidence in technology and hinder its development.

Beyond protecting users' privacy interests, the SCA also has another purpose that is clearly reflected in its legislative history—both the House and Senate reports explain that the lack of privacy protection “may unnecessarily discourage potential customers from using innovative communications systems.” (Sen.Rep., *supra*, at p. 5; accord, H.R.Rep., *supra*, at pp. 19, 65-66.) Similarly, it may

¹¹ Notably, Penal Code section 1326 does not have provisions comparable to the ones the SCA has to provide *notice* to the user for requests for certain communications. (See 18 U.S.C. § 2703(b)(1)(B) [contents stored for more than 180 days may be obtained via either a search warrant or a governmental subpoena “with prior notice to the subscriber or customer”].)

“discourage American businesses from developing new innovative forms of telecommunications and computer technology.” (Sen.Rep. *supra*, at p. 5.) During congressional hearings, industry witnesses testified as to their worries about protecting growth and development in their technological industries. (See Remarks of Sen. Leahy, 132 Cong. Rec. 7992 (1986) [introducing a version of the ECPA, Senator Patrick Leahy noting: “[Industry groups who testified before subcommittee hearings] also pointed out that the absence of such privacy protections may be inhibiting further technological development in this country and that enactment of such privacy protections will encourage the full use of modern computer technology available in America today”].)¹² The OTA report expressed the same concern. (See Federal Government Information Technology, *supra*, at p. 48 [“some believe security and privacy issues are critical to the widespread acceptance of electronic mail as a communications medium”].) As the Court of Appeal in *O’Grady* aptly explained, “[i]t would hardly be irrational of Congress to deflect such hazards by denying . . . discovery of stored messages and relegating . . . litigants to such discovery as they can obtain from or through their adversaries. On the contrary,

¹² See also, e.g., Hearings before House Com. on Judiciary, Subcom. of Courts, Civil Liberties, and the Administration of Justice, 99th Cong., 1st and 2d Sess., p. 29 (1986) (hereafter House Hearings) (Mr. Quigley (representing Cellular Telecommunications Industry Association): the ECPA “will encourage the continued growth and development of new and more effective means of communication”); *id.* at pp. 38-39 (Mr. Quigley: “no question that the expectation [of the privacy of communication] is there today, that the industry will benefit, proliferate with further assurances of privacy”).

Congress could reasonably conclude that to permit . . . discovery of stored messages from service providers without the consent of subscribers would [be] . . . too great a cost to digital media and their users.” (*O’Grady, supra*, 139 Cal.App.4th at pp. 1446-1447.)

Today’s users of service providers such as Facebook continue to find it important to be able to control third party access to their private communications. (Ante, pp. 24-25.) Moreover, today’s service providers and regulators continue to find it important to empower those users with control over their personal data and to make informed choices about that data. For instance, the National Telecommunications and Information Administration has reported that many Americans refrain from participating in online activities if they have privacy concerns, and that “for the Internet to grow and thrive, users must continue to trust that their personal information will be secure and their privacy protected.” (Goldberg, National Telecommunications and Information Administration, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities* (May 13, 2016) <<https://bit.ly/27jJfSX>> [as of May 10, 2018].)¹³ One business consulting group warns that “consumer trust converts into bottom-line benefits; in our study, half of

¹³ See also, e.g., Internet Policy Task Force, Department of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010) p. 74 <<https://bit.ly/2K80Oyt>> (as of May 10, 2018) (recommending review of the ECPA to ensure that as technology changes occur with the arrival of cloud computing and location-based services, the ECPA “continues to appropriately protect individuals’ expectations of privacy and effectively punish unlawful access to and disclosure of consumer data”).

respondents say they are willing to pay a premium for products and services from companies they trust” and that “[p]rivacy and security form the basis of trust.” (Bahl, Cognizent, *The Business Value of Trust* (May 2016), pp. 4, 6 <<https://cogniz.at/2oSvv4y>> [as of May 10, 2018].)

Touchstone’s request to weaken the SCA’s prohibition against disclosure of user communications thus runs directly contrary to the SCA’s central purposes and modern users’ concerns. Opening up users to the possibility that their communications will be disclosed to private individuals in a new manner outside of the SCA would erode their trust in the technology platforms they currently rely on, and chill their communications on those platforms. This is especially true given that they would have good reason to think that individuals involved in litigation would harness this power with little self-restraint, and perhaps even with malice. (See *Krinsky v. Doe 6* (2008) 159 Cal.App.4th 1154, 1167 [litigants can use subpoenas on service providers to “ ‘harass, intimidate or silence’ ” others who speak on the Internet].) Criminal defendants in particular could routinely issue subpoenas to service providers to obtain the communications content of victims, witnesses, confidential informants, and even law enforcement officers, because all of that information could potentially increase their leverage in plea negotiations.

Weakening the SCA’s prohibition against disclosure would also overturn users’ settled expectations. Facebook’s law enforcement guidelines, for instance, explain to its more than 200

million monthly active North American users¹⁴ that a warrant is “required to compel the disclosure of the stored contents of any account.” (Facebook, *Information for Law Enforcement Authorities* <<https://bit.ly/2G0Uzty>> [as of May 10, 2018]; see also Twitter, *Guidelines for Law Enforcement* <<https://bit.ly/2IbM00W>> [as of May 10, 2018] [similar].) It makes little sense for the judiciary to overturn these expectations and erode users’ privacy protections on an ad hoc basis, and outside of the legislative process. (See *O’Grady, supra*, 139 Cal.App.4th at p. 1443 [“The treatment of rapidly developing new technologies profoundly affecting not only commerce but countless other aspects of individual and collective life is not a matter on which courts should lightly engraft exceptions to plain statutory language without a clear warrant to do so”].)

IV. Allowing direct disclosure of user communications would be unduly burdensome on providers.

The SCA’s purpose of encouraging the development of new technologies is also served by Congress’s choice not to burden service providers with private requests for user communications from individuals involved in either civil or criminal litigation. (See *O’Grady, supra*, 139 Cal.App.4th at p. 1446 [noting that “civil subpoenas are often served on service providers and that compliance with them would impose severe administrative burdens,

¹⁴ See United States Securities and Exchange Commission, Facebook First Quarter 2018 Form 10-Q, p. 25 <<https://bit.ly/2K8GrRs>> [as of May 10, 2018].

interfering with the manifest congressional intent to encourage development and use of digital communications”].)

Responding to routine subpoena requests from private individuals is not 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 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 cost would not just involve the technological costs of searching, categorizing, compiling, and delivering data. It would also require human expertise. For instance, service providers would need to analyze data requests, narrowly tailor required responses to the requests, and resist them where appropriate, just as they currently do for government requests. (See, e.g., Apple, *Report on Government and Private Party Requests for Customer Information: January 1- June 30, 2017*, p. 2 <<https://apple.co/2xO5fLM>> [as of May 10, 2018] [hereafter *Apple Report*] [“Our legal team reviews requests received to ensure that the requests have a valid legal basis. If they do, we comply with the requests and provide the narrowest possible set of data responsive to the request. If we determine a request does not have a valid legal basis, or if we consider it to be unclear, inappropriate or over-broad, we challenge or reject it.”].) This 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 data where they were prohibited from doing so, other than in “good faith reliance” on, e.g., a court order. (See § 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.)

In addition, the burden on service providers would be even higher if providers were also legally compelled to respond to court orders compelling users to consent to data disclosures by the service providers.¹⁵ In that case, providers would need to expend even more resources to verify the consent. This would also potentially require them to develop more stringent account-verifying procedures and, further eroding users’ privacy interests and trust, collect more data from users in order to satisfy those procedures.

Nor would the costs incurred by service providers to respond to private individual subpoena requests for user communications be reimbursed. The SCA provides for reimbursement of costs for data access if the costs were “reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information,” including those costs “due to

¹⁵ As Facebook argues, service providers should not be compelled to do so, even if it would be valid for courts to order users consent to disclosure. (ABOM 31-34.)

necessary disruption of normal operations” of the provider. (§ 2706(a).) However, the reimbursement provision is expressly limited to reimbursement by a “governmental entity.” (*Ibid.*)

Currently, Facebook and other service providers already expend substantial resources responding to government subpoenas and search warrants allowed under the SCA. For instance, from January 2017 until June 2017 alone, Facebook received 32,716 law enforcement requests for data on 52,280 user accounts and produced data in response to 85 percent of those requests. (Facebook Transparency Report for the United States: Law Enforcement Requests for Data <<https://bit.ly/2jM2TVz>> [as of May 10, 2018].) Of those, 19,393 involved search warrants, and 7,632 involved subpoenas. (*Ibid.*) It also received 48,836 preservation requests for 84,497 user accounts. (*Ibid.*) Other service providers are similarly heavily burdened.¹⁶ If private individuals—whose interests in others’ data can be substantially broader and more disparate than prosecutors and law enforcement—were allowed to

¹⁶ See, e.g., *Apple Report, supra*, p. 7 <<https://apple.co/2xO5fLM>> (as of May 10, 2018) (1,711 requests with 84 percent response rate); Dropbox, *Transparency Reports* <<https://bit.ly/2KMLXdH>> (as of May 10, 2018) (in January to June 2017, 1,420 search warrant or subpoena requests); Google, *Transparency Report for United States: Requests for User Information* <<https://bit.ly/2KaALXp>> (as of May 10, 2018) (16,054 requests for 34,747 user accounts, with an 82 percent response rate); Oath, *Transparency Report for the United States: Law Enforcement Data Requests* <<https://bit.ly/2jKGZ54>> (as of May 10, 2018) (5,955 requests for 10,968 user accounts, with some data disclosed for 5,045 requests); Twitter, *Transparency Report for United States: Information Requests January to June 2017* <<https://bit.ly/2K9OLAt>> (as of May 10, 2018) [2,111 requests for 4594 user accounts, with 77 percent response rate].


seek user communication disclosures from these service providers via subpoena, the floodgates would crash open. Amici submit that this Court should not promote this result.

CONCLUSION

For the reasons explained above, the judgment of the Court of Appeal should be affirmed.

May 11, 2018

HORVITZ & LEVY LLP
JEREMY B. ROSEN
STANLEY H. CHEN

By: 
Stanley H. Chen

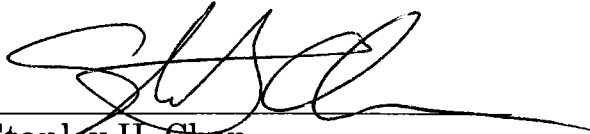
Attorneys for Amici Curiae
**APPLE INC., GOOGLE INC., OATH
INC., TWITTER, INC., AND
CALIFORNIA CHAMBER OF
COMMERCE**

CERTIFICATE OF WORD COUNT

(Cal. Rules of Court, rule 8.504(d)(1).)

The text of this brief consists of 5,515 words as counted by the Microsoft Word version 2010 word processing program used to generate the brief.

Dated: May 11, 2018



Stanley H. Chen

PROOF OF SERVICE

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, California 91505-4681.

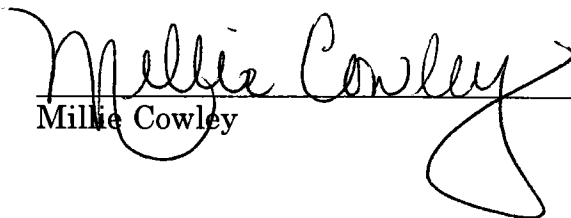
On May 11, 2018, I served true copies of the following document(s) described as **APPLICATION TO FILE AMICI CURIAE BRIEF; AMICI BRIEF OF APPLE INC., GOOGLE INC., OATH INC., TWITTER, INC. AND CALIFORNIA CHAMBER OF COMMERCE IN SUPPORT OF PETITIONER FACEBOOK, INC.** on the interested parties in this action 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 the 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.

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

Executed on May 11, 2018, at Burbank, California.


Millie Cowley

SERVICE LIST
Facebook v. Superior Court (Touchstone)
Case No. S245203

James G. Snell
Christian Lee
Perkins Coie LLP
3150 Porter Drive
Palo Alto, CA 94304

Attorneys for Petitioner
Facebook, Inc.

Joshua Seth Lipshutz
Gibson, Dunn & Crutcher LLP
555 Mission Street
San Francisco, CA 94105

Attorneys for Petitioner
Facebook, Inc.

Michael J. Holecek
Gibson Dunn & Crutcher LLP
333 South Grand Avenue
Los Angeles, CA 90071-1512

Attorneys for Petitioner
Facebook, Inc.

Katherine Ilse Tesch
Office of the Alternate Public Defender
450 B Street, Suite 1200
San Diego, CA 92101

Attorneys for Real Party in Interest
Lance Touchstone

Michael C. McMahon
Office of the Ventura County Public
Defender
800 S. Victoria Avenue, Suite 207
Ventura, CA 93009

Attorneys for Amici Curiae
California Public Defenders Association
and Public Defender of Ventura County

Donald E. Landis
The Law Office of Donald E. Landis, Jr.
P.O. Box 221278
Carmel, CA 93922

Attorneys for Amicus Curiae
California Attorneys for Criminal Justice

Stephen Kerr Dunkle
Sanger Swysen & Dunkle
125 East De La Guerra Street, Suite 102
Santa Barbara, CA 93101

Attorneys for Amicus Curiae
California Attorneys for Criminal Justice

John T. Philipsborn
Law Offices of J.T. Philipsborn
Civic Center Building
507 Polk Street, Suite 350
San Francisco, CA 94102

Attorneys for Amicus Curiae
California Attorneys for Criminal Justice

California Court of Appeal
Fourth Appellate District, Div. One
750 B Street, Ste. 300
San Diego, CA 92101-8196

Case No. D072171
Served Through Truefiling

Hon. Kenneth K. So
Central Courthouse
1100 Union Street, 20th Floor
Dept. 2004
San Diego, CA 92101

Case No. SCD268262