

SUPREME COURT COPY

No. S230051

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

FACEBOOK, INC., INSTAGRAM, LLC, AND TWITTER, INC.,
Petitioners,

v.

THE SUPERIOR COURT OF SAN FRANCISCO COUNTY,
Respondent.

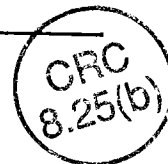
SUPREME COURT
FILED

FEB 7 2017

DERRICK D. HUNTER AND LEE SULLIVAN
Real Parties in Interest

Jorge Navarrete Clerk

Deputy



After a Published Opinion by the Court of Appeal,
First Appellate District, Division Five,
Case No. A144315

From the Superior Court, San Francisco County
Case Nos. 13035657 and 13035658
Judge Bruce Chan, Judge Presiding

**SUPPLEMENTAL *AMICUS CURIAE* BRIEF OF GOOGLE INC.
IN SUPPORT OF PETITIONERS**

Donald M. Falk (SBN 150256)
MAYER BROWN LLP
Two Palo Alto Square
3000 El Camino Real
Palo Alto, CA 94306
(650) 331-2000

Attorney for Amicus Curiae

TABLE OF CONTENTS

	Page
INTEREST OF THE <i>AMICUS CURIAE</i>	1
INTRODUCTION AND SUMMARY OF ARGUMENT	1
ARGUMENT	2
A. The SCA Leaves No Room To Infer Additional Limits On Its Scope.	2
B. The Proposed Limitation To “Communications That Were, When Sent, Configured To Be Private—i.e., Restricted To ‘Followers’ Or ‘Friends’”—Is Impracticable.....	5
C. Public Status Is An Inaccurate Gauge Of User Consent For Provider Disclosure.	6
D. Any Presumption Of Consent Would Have To Account For The User’s Ability To Reclaim Privacy Under Fourth Amendment Jurisprudence.	9
E. The Prudent Course Is To Apply And Enforce The Anti-Disclosure Provisions As Written.	11
CONCLUSION	12

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Illinois v. Andreas</i> (1983) 463 U.S. 765	9, 10
<i>Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.</i> (2d Cir. 2016) 829 F.3d 197.....	3, 4
<i>Murphy v. Spring</i> (N.D. Okla. 2014) 58 F.Supp.3d 1241	10
<i>Negro v. Superior Court</i> (2014) 230 Cal.App.4th 879	3
<i>People v. Loveless</i> (1980) 80 Ill.App.3d 1052, 400 N.E.2d 540	9
<i>People v. Riegler</i> (1984) 159 Cal.App.3d 1061	10
<i>United States v. Cotterman</i> (9th Cir. 2013) 709 F.3d 952	9
<i>United States v. Ramsey</i> (1977) 431 U.S. 606	9
 Statutes and Rules	 Page(s)
18 U.S.C. § 2510	5
18 U.S.C. § 2511(1)	2
18 U.S.C. § 2511(2)(g)(i).....	1, 2, 4
18 U.S.C. § 2701	2
18 U.S.C. § 2702	1, 2
18 U.S.C. § 2702(a)(1)	1
18 U.S.C. § 2702(a)(2)	1
18 U.S.C. § 2702(b)	3
18 U.S.C. § 2702(b)(3).....	3, 7
18 U.S.C. § 2711	5

TABLE OF AUTHORITIES
(continued)

Statutes and Rules	Page(s)
Cal. Rules of Court 8.520(f)(4)	1
Other Authorities	Page(s)
H.R. Rep., 2d Sess., No. 99-647 (1986).....	4
Sen. Rep., 2d Sess., No. 99-541 (1986)	4
Sam Thielman, <i>Yahoo hack: 1bn accounts compromised by biggest data breach in history</i> (Dec. 15, 2016) The Guardian, available at https://www.theguardian.com/technology/2016/dec/14/yahoo- hack-security-of-one-billion-accounts-breached	7

INTEREST OF THE *AMICUS CURIAE*

The interest of Google Inc. in this case is fully explained in its initial *amicus curiae* brief. Google submits this brief in response to this Court’s order of December 21, 2016.¹

Google is acutely interested in the question presented in that order. Imposing nonstatutory limits on the scope of providers’ duty not to divulge electronic communications under the Stored Communications Act, 18 U.S.C. § 2702, would raise significant practical problems of compliance and enforcement while impairing users’ confidence in the privacy of their communications. In particular, a legal standard that used past accessibility to the public to negate the provider’s duty would be unfair to users and impractical to administer.

INTRODUCTION AND SUMMARY OF ARGUMENT

The Stored Communications Act (SCA) leaves no room to add nonstatutory limitations to an electronic communication service provider’s duty not to “divulge to any person or entity the contents of a communication” that is stored, carried, or maintained on that service. (18 U.S.C. § 2702(a)(1); see *id.* § 2702(a)(2).) The provision cited in this Court’s supplemental briefing order excludes a “communication system” that is configured so that such electronic communication is readily accessible to the general public—but only as a basis for liability for “*intercept[ing]* or *access[ing]*” an electronic communication under the SCA. (18 U.S.C. § 2511(2)(g)(i) [emphasis added].) In contrast, the SCA section at issue here, 18 U.S.C. § 2702, prohibits *divulging* a

¹ No party and no counsel for any party in this case authored the proposed amicus brief in whole or in part, or made a monetary contribution intended to fund the preparation or submission of the brief. No person or entity made a monetary contribution intended to fund the preparation or submission of the brief, other than the amici curiae and their counsel in this case. (See Cal. Rules of Court, rule 8.520(f)(4).)

communication. The exclusion in Section 2511(2)(g)(i) says nothing about the duty not to divulge.

As petitioners point out, the only pertinent statutory exception to the provider duty is that for user consent. For the reasons explained below, user consent should not be inferred from privacy settings, particularly not past privacy settings that may have exposed a communication to public access in the past but no longer do so. That inference is not justified by the statute's text or legislative history, or by users' actual intent. And making provider duties turn on the past privacy settings of communications would make compliance with those duties uncertain and difficult. Accordingly, the Court should construe the SCA according to its terms, without artificially limiting providers' obligation to protect users' privacy.

ARGUMENT

A. The SCA Leaves No Room To Infer Additional Limits On Its Scope.

1. The Electronic Communications Privacy Act, which includes the SCA, protects the privacy of electronic communications in three ways. Two separate provisions prohibit “any person” from “intercept[ing]” an electronic communication or “intentionally access[ing]” an electronic communication “without authorization.” (18 U.S.C. § 2511(1); *id.* § 2701.) A third restriction—the only one at issue here—prohibits electronics services providers from “divulg[ing]” communications that are stored or carried on their systems. (*Id.* § 2702.)

The supplemental briefing order suggests that the provision prohibiting service providers from “divulg[ing]” users' communications might be construed to exclude communications “that were, when sent, configured to be public.” In support of this proposed restriction, the order cites 18 U.S.C. § 2511(2)(g)(i), which states that it shall not be unlawful “to *intercept* or *access* an electronic communication made through an

electronic communication system that is configured so that such electronic communication is readily accessible to the general public” (emphasis added). By its plain language, that exemption applies only to liability for accessing or intercepting communications, not to a service provider’s duty not to *divulge* users’ communications.

2. Congress did provide eight express exceptions to providers’ duty not to divulge. (See 18 U.S.C. § 2702(b)). The only exception arguably related to public accessibility allows a provider to divulge a communication with the “lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service.” (*Id.* § 2702(b)(3).)

Accordingly, a conclusion that publicly accessible messages do not fall within the providers’ duty would effectively infer consent from privacy settings. But concepts of implied consent are misplaced in this context. Although it did not ultimately decide the issue, the Court of Appeal properly “question[ed] the soundness of ... a construction of the [SCA]” that would permit a court to infer consent from a party’s conduct with respect to a message “for purposes of compelling a provider to disclose stored messages.” (*Negro v. Superior Court* (2014) 230 Cal.App.4th 879, 891.) The *Negro* court also criticized efforts to rely on antiwiretapping provisions aimed at third-party interception as a basis to recognize an implied consent principle with respect to *provider* duties. (*Id.* at 891 n.2.)

3. On the contrary, this Court should construe the statutory terms in light of the SCA’s “focus ... on the need to protect users’ privacy interests.” (*Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.* (2d Cir. 2016) 829 F.3d 197, 218.) That focus is reflected in the SCA’s structure: providers’ “primary obligations ... protect the electronic communications”;

“[d]isclosure is permitted only as an exception to those primary obligations.” (*Ibid.*)

The legislative history confirms that Congress’s primary motivation was “to protect the privacy of our citizens” by imposing federal statutory presumptions that codify citizens’ expectations of privacy in “new forms of telecommunications and computer technology.” (Sen. Rep. No. 99-541, 2d Sess., p.5 (1986)). That history also makes clear that the exception to liability for access to or interception of publicly accessible communications now codified in Section 2511(2)(g)(i) is limited to communications that use entire *systems* that are configured to be accessible to the public (as the statutory text says). Congress did not intend a communication-by-communication analysis of privacy settings, but rather intended “an objective standard of design configuration,” giving as examples of pertinent systems “the stereo subcarrier used in FM broadcasting or data carried ... to provide closed-captioning of TV programming for the hearing-impaired.” (*Id.* at 18.) Indeed, the House Report makes clear that “nothing carried by wire is ‘readily accessible to the general public’” (H.R. Rep. No. 99-647, 2d Sess., p. 41 (1986)), which would exclude the social media postings at issue here.

In addition, the legislative history of the prohibition on unauthorized *access* to electronic communications suggests that its scope is limited to “electronic or wire communications that are not intended to be available to the public.” (Sen. Rep. 99-541, at 35.) But the legislative history of the provision prohibiting carriers from *divulging* communications reflects no such limit. (See *id.* at 36-38.)

Both the Senate and House Reports declared that “[p]rivacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.” (Sen. Rep. 99-541, at 5; H.R. Rep. No. 99-647, at 19.) An interpretation of the SCA that would make providers’ duty to

protect user communications contingent upon the history of physical privacy settings would contradict this stated policy. More important, inferring one nonstatutory limit on providers' duty to protect users' privacy would open the door to additional inferential limits that cumulatively would negate the statute's privacy protections.

B. The Proposed Limitation To “Communications That Were, When Sent, Configured To Be Private—i.e., Restricted To ‘Followers’ Or ‘Friends’”—Is Impracticable.

Even if the SCA could be construed (in the words of the December 21 Order) to permit providers to divulge stored “communications that were, when sent, configured to be public,” that limitation would present significant practical difficulties. The SCA should not be implicated with respect to communications that are currently configured to be public. Those communications are directly accessible to criminal defendants, civil litigants, and everyone else. So this proposed dividing line would have practical application only to communications that are no longer publicly accessible, but that were “configured to be public” at some time in the past.

The first problem is one of recordkeeping and storage. Providers do not routinely maintain records of past privacy settings for each post or message. Lacking such records, it would be impossible to determine the privacy configuration that applied when a communication was posted or sent.

In addition, the proposed limit on the divulgement prohibition is uncertain because the statute does not define “sent.” (See 18 U.S.C. § 2711 [incorporating 18 U.S.C. § 2510 and providing additional definitions].) “When sent” might mean only the original posting of a message. In that case, as noted above, few if any service providers would have the means to establish the original privacy settings on a post or message if the settings had changed.

In the alternative, a communication might be considered “sent” anew whenever its privacy settings were changed. That definition would raise the question whether the communication’s most recent privacy settings alone would determine when it was “sent,” or whether a communication for which privacy settings had changed would be treated as a series of communications that were “sent” upon each setting change. If only the most recent privacy settings count in the analysis, a third party already would have access to any communication configured to be publicly accessible without any need to breach the SCA anti-divulgement provisions. But a definition under which a communication was “sent” whenever its settings changed would produce the same, likely insuperable administrative problems as any other legal test that depended on a communication’s superseded privacy settings. And the problems would not be merely administrative. Treating a communication as “sent” upon every change in privacy settings could mean that, if communications were no longer “restricted to ‘followers’ or ‘friends’” because of a password breach or other security failure, the communications might be treated as “configured to be public” when “sent” at that time. Under that interpretation, providers might have to prove that a particular account had never been breached in order to show that the post was never “configured to be public.” That would reverse the presumption of privacy that the terms of the SCA impose, and that the legislative history indicates was Congress’s intent.

C. Public Status Is An Inaccurate Gauge Of User Consent For Provider Disclosure.

The only statutory exception that could conceivably allow providers to divulge users’ electronic communications based on their privacy configuration is the exception permitting disclosure “with the lawful consent of the originator[,] ... addressee[,] ... intended recipient of [a]

communication, or the subscriber in the case of remote computing service.” (18 U.S.C. § 2702(b)(3).) For many reasons, however, privacy settings—and especially *past* privacy settings—are a poor gauge of actual user consent to disclosure.

1. To begin with, equating exposure of a communication to the public with consent under the SCA would raise significant privacy issues. Password breaches and credential disclosures can lead to changes in security settings. Then a post may be picked up by web crawler that would make the post widely (if not well-nigh universally) accessible.

The recently revealed breach of a billion Yahoo accounts provides an apt example. (See, *e.g.*, Sam Thielman, *Yahoo hack: 1bn accounts compromised by biggest data breach in history* (Dec. 15, 2016) *The Guardian*, available at <https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached>.) That hack reportedly exposed passwords and similar information that would allow the hackers to indirectly commandeer the privacy settings on Yahoo accounts (and potentially other accounts where Yahoo users used the same password). The hack also involved forged “cookies,” which normally permit a user to remain signed into an account without logging in upon every visit to a website, but that, when forged, apparently could permit a hacker direct access to accounts and account settings.

Public accessibility that results from a breach flatly contradicts user intention. Inferring “lawful consent” to disclosure from such a circumstance would conflict with both common sense and the privacy-focused legislative policy underlying the SCA.

2. A social media user also may erroneously post a communication using a public setting while believing that a post is limited to a private group. For example, with some services, when a user optimizes a group for a particular post, the same group becomes the default for the

next post. That is, the system presumes that each post should duplicate the privacy configuration for the immediately preceding post. The user may or may not detect and correct the setting. But the user certainly has not validly consented to the service provider's divulgement of the communication.

Many other factors may result in inadvertent user errors in privacy configurations for particular communications. For example, some users may overlook interface changes and fail to recognize settings that are displayed differently than before. And changes in the content and character of privacy settings may lead to similar results: a user may misapprehend how widely a communication will be exposed.

A standard that tethers service providers' anti-divulgement obligations to privacy settings on particular communications accordingly would require some allowance—perhaps a grace period—for user correction of privacy-setting mistakes. After all, if the user corrects a privacy-configuration mistake soon enough, no one may have seen the post while it was accessible to the public. It would be grossly unfair if such errors nullified the obligation of service providers not to divulge users' communications.

3. Finally, additional, complicated issues would arise from unusual settings and uses. The contemporary Internet provides an almost endless array of communications modalities and privacy settings. For example, a blogger may configure a particular post to be unlisted. There would be no privacy protections; anyone who had the universal resource locator (url) for the blog post could access it. But no one could find the post without the url in hand. How would a provider or a court determine whether the federal divulgement prohibition applied to an unlisted blog post? Any effort to infer the nature and scope of the user's consent to divulgement would be hopelessly uncertain in that and similar circumstances.

D. Any Presumption Of Consent Would Have To Account For The User's Ability To Reclaim Privacy Under Fourth Amendment Jurisprudence

Any presumption of consent to divulgement that rested on configuration to be publicly accessible would have to be applied in light of Fourth Amendment jurisprudence that allows a citizen to reclaim a privacy interest. The SCA's statutory privacy protections extend beyond the limits of the Fourth Amendment. At a minimum, therefore, the statutory protections should reflect a solicitude for privacy that equals the constitutional standard.

For example, a person who leaves her "coat on a table in a busy tavern" may lose her reasonable expectation of privacy in its contents. (*People v. Loveless* (1980) 80 Ill.App.3d 1052, 1054, 400 N.E.2d 540, 542.) But she can regain that expectation simply by saying, "Hey, ... that's my coat," when a police officer picks it up. (*Id.* at 1055, 400 N.E.2d at 542; see *id.* at 1055-56; 400 N.E.2d at 543-44 [suppressing fruits of search].)

It is likewise well-established that an individual temporarily loses any reasonable expectation of privacy in his or her belongings when crossing an international border. (*E.g.*, *United States v. Ramsey* (1977) 431 U.S. 606, 616.) But that loss of privacy persists only during the border crossing; once the individual has "cleared the border," he "regain[s] an expectation of privacy in [his] accompanying belongings (*United States v. Cotterman* (9th Cir. 2013) 709 F.3d 952, 961 (en banc); see *id.* at 974 n.4 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment).)

Similar principles underlie the U.S. Supreme Court's recognition that an individual can regain a reasonable expectation of privacy in the contents of a container previously subject to a lawful search if the "gap in surveillance" is long enough. (*Illinois v. Andreas* (1983) 463 U.S. 765,

772–73.) The Court held that the recipient of a package known to contain marijuana *could* have regained a reasonable expectation of privacy in the contents when he took the package into his home. (*Id.* at 772–73.) Applying a multi-factor contextual analysis, however, the Court found the 45-minute gap in that case insufficient. Applying *Andreas* in another case, however, the Court of Appeal concluded that a two-and-one-half-hour period while a box previously known to contain contraband was inside a house and then inside a car *did* re-establish a reasonable expectation of privacy. (See *People v. Riegler* (1984) 159 Cal.App.3d 1061, 1065–67, 1069.)

The same principles of revived privacy expectations have been applied to the search of an email account. In *Murphy v. Spring* (N.D. Okla. 2014) 58 F.Supp.3d 1241, 1269, the court denied summary judgment against a civil rights claim alleging a Fourth Amendment violation, on the ground that the plaintiff could regain a reasonable expectation of privacy in her Yahoo email account. The defendants, the plaintiff’s former supervisors, contended that she lacked a reasonable expectation of privacy in the account because her password was written on a shared department calendar. (*Ibid.*) Even if the plaintiff had “somehow acquiesced to her supervisors using her private email account for work-related purposes while she assisted them,” the court observed, “the accessing” claimed to violate the Fourth Amendment “took place after [the plaintiff’s] suspension and for the purpose of finding information related to [her] upcoming termination hearing.” (*Ibid.*) That is, even if the plaintiff temporarily waived any reasonable expectation of privacy for one limited purpose, her expectation of privacy in her data could revive when that purpose no longer could be served.

Users of social media and other electronic communications platforms likewise can regain an expectation of privacy when they change the settings on their communications. Whether a communication was

exposed to the public through a security breach or inadvertence, or whether the user simply had a change of heart, once a communication is no longer accessible to the public, the user has a reasonable expectation of privacy in its contents. That expectation is fully subject to the protections of the SCA.

E. The Prudent Course Is To Apply And Enforce The Anti-Disclosure Provisions As Written.

Real Parties may believe that the text of the SCA is obsolete, but their remedy is with Congress, not the state and federal courts. Real Parties (RP Supp. Br. 7-8) make crystal clear that an exception for “public” status could soon swallow most of the SCA’s protections. Real Parties give away their game when they contend that any post shared with a large number of people is public—and therefore unprotected by the anti-divulgement provisions of the SCA—because someone can take a screenshot of it and disseminate it further without being limited by the original privacy settings. (RP Supp. Br. 7-14.) If Real Parties’ premise were correct, however, a communication shared with only one person would be equally public because a single recipient could share a private communication with the world (and some recipients do). A host does not lose her reasonable expectation of privacy in her home by inviting 50 visitors, any of whom might steal something. The ability to share an electronic communication accordingly cannot be the basis for removing privacy protections from content posted with less-than-public privacy settings.

Whether or not the Fourth Amendment would protect an electronic communication from government search, the SCA takes providers out of the equation as a source of information unless one of the enumerated statutory exceptions applies. As we explained in our principal amicus brief (at pp. 5-6), disclosure of stored communications must proceed through a user or law enforcement agency to whom a provider may lawfully divulge communications stored on its system.

CONCLUSION

The decision of the Court of Appeal should be affirmed.

Dated: February 6, 2017

Respectfully submitted.

Donald M. Falk (SBN 150256)
MAYER BROWN LLP
Two Palo Alto Square
3000 El Camino Real
Palo Alto, CA 94306
(650) 331-2000

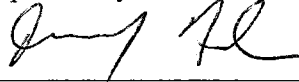
Attorney for Amicus Curiae .

CERTIFICATE OF WORD COUNT
(California Rule of Court 8.520(c)(1))

According to the word count facility in Microsoft Word 2007, this brief, including footnotes but excluding those portions excludable pursuant to Rule 8.520(c)(3), contains 3,264 words.

Dated: February 6, 2017

Respectfully submitted.



Donald M. Falk (SBN 150256)
MAYER BROWN LLP

Attorney for Amicus Curiae

I, Kristine Neale, declare as follows:

I am a resident of the State of California and over the age of eighteen years, and not a party to the within action; my business address is: Two Palo Alto Square, Suite 300, 3000 El Camino Real, Palo Alto, California 94306-2112. On February 6, 2017, I served the foregoing document(s) described as:

SUPPLEMENTAL *AMICUS CURIAE* BRIEF OF GOOGLE INC. IN SUPPORT OF PETITIONER

- By transmitting via facsimile the document(s) listed above to the fax number(s) set forth below on this date before 5:00 p.m.
- By placing the document(s) listed above in a sealed envelope with postage prepaid, via First Class Mail, in the United States mail at Palo Alto, California addressed as set forth below.
- By causing the document(s) listed above to be personally served on the person(s) at the address(es) set forth below.
- By placing the document(s) listed above in a sealed overnight service envelope and affixing a pre-paid air bill, and causing the envelope, addressed as set forth below, to be delivered to an overnight service agent for delivery.

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

*Attorney for Facebook, Inc.,
Instagram LLC and Twitter Inc.*

Jose Pericles Umali
Attorney at Law
507 Polk Street, Suite 340
San Francisco, CA 94102

Attorney for Derrick D. Hunter

Eric David Miller
John R. Tyler
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101

*Attorneys for Facebook, Inc.,
Instagram LLC and Twitter Inc.*

Susan B. Kaplan
214 Duboce Avenue
San Francisco, CA 94103

Attorney for Lee Sullivan

Janelle Elaine Caywood
Attorney at Law
3223 Webster Street
San Francisco, CA 94123

Attorney for Lee Sullivan

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

*Amicus Curiae California Public
Defenders Association & Public
Defender of Ventura County*

Donald E. Landis
Monterey County Assistant
Public Defender
11 West Alisal Street
Salinas, CA 93901

John T. Philipsborn
Law Offices of J.T. Philipsborn
507 Polk Street, Suite 350
San Francisco, CA 94012

*Amicus Curiae California Attorneys
for Criminal Justice*

Judge Bruce Chan
Superior Court, San Francisco County
850 Bryant Street
San Francisco, CA 94103

Heather Alison Trevisan
Office of the District Attorney
850 Bryant Street, Room 322
San Francisco, CA 94103

Attorney for the State of California

Jeffrey Gordon Adachi
Dorothy Katherine Bischoff
San Francisco Public Defender's
Office
555 7th Street
San Francisco, CA 94103

*Amicus Curiae San Francisco Public
Defender's Office*

David M. Porter
Office of Federal Public Defenders
801 "I" Street, 3rd Floor
Sacramento, CA 95814

Donald E. Landis
Monterey County Assistant
Public Defender
11 West Alisal Street
Salinas, CA 93901

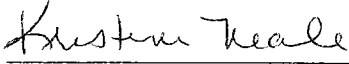
*Amicus Curiae National Association of
Criminal Defense Lawyers*

First Appellate District, Div. 5
350 McAllister Street
San Francisco, CA 94102

I am readily familiar with the firm's practice of collection and processing correspondence for mailing. Under that practice it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid in the ordinary course of business.

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

Executed on February 6, 2017, at Palo Alto, California.



Kristine Neale