

No. S230051

Supreme Court Copy

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.

DERRICK D. HUNTER AND LEE SULLIVAN

Real Parties in Interest

FILED WITH PERMISSION

SUPREME COURT

FILED

APR 12 2016

Frank A. McGuire Clerk

Deputy

CRC
8.25(b)

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

**APPLICATION OF GOOGLE INC. FOR PERMISSION TO FILE
AMICUS CURIAE BRIEF AND
AMICUS CURIAE BRIEF 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

**APPLICATION OF GOOGLE INC. FOR PERMISSION TO FILE
AMICUS CURIAE BRIEF IN SUPPORT OF PETITIONERS**

To the Honorable Tani Cantil-Sakauye, Chief Justice:

Google Inc. respectfully applies for permission to file the attached *amicus curiae* brief in support of petitioners Facebook, Inc., Instagram L.L.C., and Twitter, Inc.¹ This case presents issues of paramount importance to Google respecting the scope of the federal Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*, and the extent to which the SCA’s unequivocal statutory commands may be overridden by asserted federal constitutional rights. Google has a strong interest in the correct resolution of these issues because it provides services that qualify as “electronic communications services” and “remote computing services” within the meaning of the statute. (See 18 U.S.C. § 2711(1)-(2); *id.* § 2510(14)-(15).)

The issues in this case are of broad importance to all entities that provide electronic communications and stored computing services, whether in the form of traditional email or in the dizzying array of social media services that account for an increasing percentage of Californians’ electronic communications. Because so many Californians use those services, a decision that applied the SCA in a way that loosened the statutory prohibitions on disclosure would greatly increase the burden to Google from requests to disclose the contents of its users’ stored communications. And such a decision would undercut users’ confidence in the privacy of their communications when using those services.

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).)

Google Inc. is a technology company that offers a suite of web-based products and services to billions of people worldwide. Google's search engine processes more than 3.5 billion searches per day and more than 1 trillion searches per year. Google's Gmail service provides email for 900 million global users. Google Maps is used by more than 1 billion people each month. Google also operates a number of services that provide social media functions at least in part, including Google+, Waze, and YouTube.

Google frequently participates in matters of importance before this Court and other courts. (See, e.g., *Strauss v. Horton* (2009) 46 Cal.4th 364; *City of Hope v. Genentech Nat'l Medical Center v. Genentech, Inc.* (2008) 43 Cal.4th 375; *Halo Electronics, Inc. v. Pulse Electronics, Inc.* (U.S. argued Feb. 23, 2016, 14-1513, -1520); *Spokeo, Inc. v. Robins* (U.S. argued Nov. 2, 2015, 13-1339); *City of Los Angeles v. Patel* (2015) 135 S.Ct. 2443.)

As explained in the proposed brief, Real Parties' erroneous contentions provide no basis to narrow or override the SCA, which serves important functions not only in protecting user privacy but also in insulating service providers from a plethora of requests for private information from user accounts. As the brief further explains, this case presents no conflict between the SCA and Real Parties' constitutional rights; Real Parties' contrary assertions depend on an unprecedented and unwarranted expansion of criminal defendants' pretrial discovery rights. More important, even if Real Parties' constitutional rights were legitimately at issue here, there is no true conflict with the SCA. If a criminal defendant made a successful threshold showing that information available only from a provider subject to the SCA was reasonably likely to contain exculpatory evidence, and that there was no other reasonable means of obtaining the information under the SCA, the court could put the prosecution to the

choice of using its superior means of gaining access to SCA-protected information and then turning over to the defendant any exculpatory evidence (including impeachment evidence) consistent with its duties under *Brady v. Maryland* (1963) 373 U.S. 83—or suffering dismissal or an adverse evidentiary finding.

CONCLUSION

The application should be granted and the accompanying *amicus curiae* brief filed.

Dated: April 6, 2016

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

TABLE OF CONTENTS

	Page
INTEREST OF THE <i>AMICUS CURIAE</i>	1
INTRODUCTION AND SUMMARY OF ARGUMENT	1
ARGUMENT	3
I. By Generally Forbidding Service Providers To Disclose Electronic Communications, The SCA Creates A Federal Statutory Privilege Against Compelled Disclosure By Providers	3
II. The SCA May Be Constitutionally Applied To Prohibit Pretrial Disclosures To A Criminal Defendant.	6
A. Criminal defendants have no federal constitutional right to investigative tools that are equal or even similar to those available to law enforcement agencies.	8
B. Criminal defendants have no constitutional right of access to third-party evidence before trial.	9
III. Public Policy Favors Upholding And Enforcing The SCA According To Its Terms.	11
A. Less restrictive means provide reasonable access to the information at issue.	11
1. A user or recipient may authorize (or may be compelled to authorize) disclosure under the SCA. ..	12
2. A decedent's account may have a successor with authority to consent to disclosure under the SCA.	13
3. The prosecutor may be put to the choice of using its investigative capabilities under the SCA to obtain and provide potential <i>Brady</i> material or else suffering dismissal or an adverse evidentiary finding.	14

TABLE OF CONTENTS
(continued)

	Page(s)
B. The unintended consequences of overriding the federal statutory privilege further weigh against finding disclosure constitutionally compelled.....	16
C. The Court should not prejudge the circumstances, if any, in which a criminal defendant’s constitutional rights would override the protections of the SCA.	18
CONCLUSION	19

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Al Noaimi v. Zaid</i> (D.Kan. 2012) 2012 WL 4758048.....	12
<i>Bower v. Bower</i> (D.Mass. 2011) 808 F.Supp.2d 348.....	12
<i>Brady v. Maryland</i> (1963) 373 U.S. 83.....	<i>passim</i>
<i>Crispin v. Christian Audigier, Inc.</i> (C.D.Cal. 2010) 717 F.Supp.2d 965	4
<i>Ehling v. Monmouth-Ocean Hospital Service Corp.</i> (D.N.J. 2013) 961 F.Supp.2d 659	12
<i>Flagg v. City of Detroit</i> (E.D. Mich. 2008) 252 F.R.D. 346.....	12
<i>FTC v. Netscape Communications Corp.</i> (N.D. Cal. 2000) 196 F.R.D. 559	18
<i>General Dynamics Corp. v. United States</i> (2011) 563 U.S. 478	15
<i>Glazer v. Fireman’s Fund Ins. Co.</i> (S.D.N.Y. 2012) 2012 WL 1197167	12
<i>Holmes v. South Carolina</i> (2006) 547 U.S. 319	10
<i>In re Crisis Connection, Inc.</i> (2011) 949 N.E.2d 789.....	10
<i>In re Subpoena Duces Tecum to AOL, LLC</i> (E.D. Va. 2008) 550 F.Supp.2d 606	12
<i>Jencks v. United States</i> (1957) 353 U.S. 657.....	15
<i>Juror Number One v. Superior Court</i> (2012) 206 Cal.App.4th 854	4, 5, 7
<i>Lafler v. Cooper</i> (2012) 132 S.Ct. 1376	11
<i>Miller v. Superior Court</i> (1999) 21 Cal.4th 883	3, 7
<i>Negro v. Superior Court</i> (2014) 230 Cal.App.4th 879	5, 6, 12

TABLE OF AUTHORITIES
(continued)

Cases	Page(s)
<i>O’Grady v. Superior Court</i> (2006) 139 Cal.App.4th 1423	<i>passim</i>
<i>ONEOK v. Learjet, Inc.</i> (2015) 135 S.Ct. 1591	6
<i>Pennsylvania v. Ritchie</i> (1987) 480 U.S. 39	10
<i>People v. Hammon</i> (1997) 15 Cal.4th 1117.....	9, 10, 18
<i>People v. Valdez</i> (2012) 55 Cal.4th 82.....	9
<i>Pitchess v. Superior Court</i> (1974) 11 Cal.3d 531	10
<i>Quon v. Arch Wireless Operating Co.</i> (9th Cir. 2008) 529 F.3d 892	4
<i>Romano v. Steelcase Inc.</i> (2010) 30 Misc.3d 426 [907 N.Y.S.2d 650].....	12
<i>Sublet v. State</i> (2015) 442 Md. 632 [113 A.3d 695]	14
<i>Swidler & Berlin v. United States</i> (1998) 524 U.S. 399	7
<i>United States v. Bagley</i> (1985) 473 U.S. 667.....	9
<i>United States v. Nixon</i> (1974) 418 U.S. 683	7
<i>United States v. Pierce</i> (2d Cir. 2015) 785 F.2d 832	13
<i>United States v. Ruiz</i> (2002) 536 U.S. 622.....	11
<i>Wardius v. Oregon</i> (1973) 412 U.S. 470	8, 10
<i>Weatherford v. Bursey</i> (1977) 429 U.S. 545.....	9, 11

TABLE OF AUTHORITIES
(continued)

Statutes and Rules	Page(s)
18 U.S.C. § 2701 <i>et seq.</i>	1
18 U.S.C. § 2702(a)(1).....	3
18 U.S.C. § 2702(a)(2).....	3
18 U.S.C. § 2702(b)(2).....	4
18 U.S.C. § 2702(b)(3).....	4, 13
18 U.S.C. § 2702(b)(6)-(8).....	4
18 U.S.C. § 2702(c).....	14
18 U.S.C. § 2702(c)(6).....	14
18 U.S.C. § 2703.....	14
18 U.S.C. § 2703(a)-(d).....	4
18 U.S.C. § 2703(c)(1)(C).....	18
Evid. Code § 1042.....	15
Other Authorities	Page(s)
https://googlepublicpolicy.blogspot.com/2013/04/plan-your-digital-afterlife-with.html	13
https://support.google.com/accounts/answer/3036546?hl=en	13
https://support.google.com/accounts/contact/deceased?hl=en	13
Orin Kerr, <i>A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It</i> (2004) 72 Geo. Wash. L. Rev. 1208.....	4

TABLE OF AUTHORITIES
(continued)

Other Authorities	Page(s)
Pub. L. No. 99-508 (Oct. 21, 1986) 100 Stat. 1860 et seq.....	5
Sen. Rep. No. 99-541, 2d Sess. (1986) reprinted in 1986 U.S. Code Cong. & Admin. News.....	5

INTEREST OF THE *AMICUS CURIAE*

Google Inc. is a technology company that offers a suite of web-based products and services to billions of people worldwide. Google's search engine processes more than 3.5 billion searches per day and more than 1 trillion searches per year. Google's Gmail service provides email for 900 million global users. Google Maps is used by more than 1 billion people each month. Google also operates a number of services that provide social media functions at least in part, including Google+, Waze, and YouTube.

Because so many Americans use those services, a decision that loosened the statutory prohibitions on disclosure in the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*, would greatly increase the burden to Google from requests to disclose the contents of its users' stored communications. A decision of that kind also would impair users' confidence in the privacy of their communications. Google accordingly has a strong interest in the correct resolution of this case.

INTRODUCTION AND SUMMARY OF ARGUMENT

Real Parties assert a conflict between the privacy protections enacted in the federal Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*, and the federal constitutional rights of criminal defendants. But the conflict is illusory.

The SCA bars disclosure of the records Real Parties seek except under circumstances that undisputedly are not present here. Under the Supremacy Clause, no provision or principle of state law can override the SCA; only a federal constitutional or statutory right can do that. Yet the Constitution does not provide criminal defendants with a right to pretrial discovery from third parties, let alone a right co-extensive with the investigative powers of law enforcement agencies of the type that Real

Parties ask this Court to recognize. There accordingly is no source of law that could outweigh the express prohibitions of the SCA.

But even if Real Parties had a constitutional right to some of the social media information they seek, the supposedly intractable difficulties could be resolved consistent with the terms of the SCA. Strong as it is, the SCA's federal policy does not prevent criminal defendants from gaining access to information that is material to their defense. As this case demonstrates, prosecutors often seek and obtain the same social media data that is of interest to the defense, and under *Brady v. Maryland* (1963) 373 U.S. 83, they must turn over to the defense any evidence that is exculpatory, including material that would help impeach prosecution witnesses. Courts evaluating similar issues have not hesitated to order account holders to consent to disclosure. Intended recipients of particular communications—whom the SCA authorizes to receive disclosure—might be similarly compelled to consent to their disclosure.

And even in the most difficult case—where the pertinent account holder is deceased or no one with the authority to consent to disclosure can be found—the SCA's provisions for access by law enforcement supply a straightforward and fair solution. Upon an adequate showing by the defense, the prosecution could be put to the choice of either (1) using its power to obtain the information from the provider, and then complying with its duties under *Brady* to provide the defense with any information that falls within the operative (and quite broad) definition of constitutionally exculpatory information, or (2) having the prosecution dismissed or (in less compelling cases) sustaining an adverse evidentiary finding or inference.

But that determination should await another day, when similar issues may be presented on a record that raises questions as to the scope of third-party evidence that a criminal defendant is entitled to obtain for use at trial. Because firmly established precedent forecloses any federal constitutional

claim to pretrial discovery beyond what must be turned over under *Brady*, and because the SCA preempts any state-law right to disclosure, this case does not require this Court to resolve the balance between the SCA and the federal constitutional rights of defendants. The decision of the Court of Appeal should be affirmed.

ARGUMENT

Once again, a litigant asks this Court to narrow or eliminate a statutory nondisclosure provision “in a manner contrary to its express terms, because federal due process compels such a result.” (*Miller v. Superior Court* (1999) 21 Cal.4th 883, 901.) Though the requesters this time are criminal defendants rather than prosecutors, the result should be the same. Because in fact “there is no such conflicting right presented in this case” (*ibid.*), the Court should not limit the operation of the SCA, but instead should enforce it according to its terms and affirm the judgment below.

I. BY GENERALLY FORBIDDING SERVICE PROVIDERS TO DISCLOSE ELECTRONIC COMMUNICATIONS, THE SCA CREATES A FEDERAL STATUTORY PRIVILEGE AGAINST COMPELLED DISCLOSURE BY PROVIDERS.

The touchstones of this case are the text and purposes of the SCA. The statute’s text is indisputably clear: “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” (18 U.S.C. § 2702(a)(1).) A similar prohibition applies to a provider of “remote computing service to the public,” who “shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service” that was received from “a subscriber or customer of such service.” (*Id.* § 2702(a)(2); see *O’Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 1443 [noting that SCA “clearly prohibits any disclosure of stored email other than as

authorized by enumerated exceptions”].) As the Ninth Circuit has explained, “[g]enerally, the SCA prevents ‘providers’ of communication services from divulging private communications to certain entities and/or individuals.” (*Quon v. Arch Wireless Operating Co.* (9th Cir. 2008) 529 F.3d 892, 900, cert. denied in pertinent part *sub nom. USA Mobility Wireless, Inc. v. Quon* (2009) 558 U.S. 1091 [130 S.Ct. 1011, 175L.Ed.2d 618], rev’d in part on other grounds *sub nom. City of Ontario v. Quon* (2010) 560 U.S. 746, 755 [130 S.Ct. 2619, 177 L.Ed.2d 216] [citing Orin Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It* (2004) 72 Geo. Wash. L. Rev. 1208, 1213].)

There likewise is no dispute that the social media providers here—on whose networks communications are accessible to a limited number of “friends” or addressees—fall under either or both definitions. (Cf., e.g., *Juror Number One v. Superior Court* (2012) 206 Cal.App.4th 854, 862-63; *Crispin v. Christian Audigier, Inc.* (C.D.Cal. 2010) 717 F.Supp.2d 965.) (Unless otherwise indicated, the remainder of this brief uses “providers” to encompass both providers of electronics communications services and providers of remote computing services.)

The SCA’s broad prohibitions are subject to narrow exceptions. Apart from disclosures incident to delivering the communication to its addressees, communications may be disclosed only “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” (18 U.S.C. § 2702(b)(3)); to law enforcement agencies or (in cases of emergency) other government entities under narrow and specified circumstances (see *id.* §§ 2702(b)(2), (6)-(8)); or pursuant to a search warrant, a court order in support of a criminal investigation, or an administrative subpoena (see *id.* § 2703(a)-(d)). Again, there is no dispute

that criminal defendants seeking discovery of third parties' accounts do not fall within any of these exceptions,

The SCA's clear prohibition on disclosure by service providers creates a federal statutory privilege that—with its few enumerated exceptions—lodges the right to disclose stored electronic communications in users. “The SCA's requirement of ‘lawful consent’ is manifestly intended to invest users with the final say regarding disclosure of the contents of their stored messages while limiting the burdens placed on service providers by the Act.” (*Negro v. Superior Court* (2014) 230 Cal.App.4th 879, 896.)

Thus, as the *Negro* court understood, two pertinent policies underlie the SCA: (1) to protect users of electronic communications from unwarranted intrusions on their privacy, (2) to encourage the provision of electronic communications services and remote computing services by protecting providers from an otherwise limitless burden of responding to requests to disclose their users' communications. The Senate Report accompanying the SCA made both purposes clear. The Act sought “to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs.” (Sen. Rep. No. 99–541, 2d Sess. (1986) reprinted in 1986 U.S. Code Cong. & Admin. News, p. 3557.) As the Court of Appeal has observed, “Congress passed the SCA as part of the Electronic Communications Privacy Act of 1986 (Pub.L. No. 99–508 (Oct. 21, 1986) 100 Stat. 1860 et seq.) to fill a gap in the protections afforded by the Fourth Amendment.” (*Juror Number One*, *supra*, 206 Cal.App.4th at 860.) And it also sought to dispel the legal uncertainty and potential burdens that might “discourage American businesses from developing new innovative forms of telecommunications and computer technology.” (Sen. Rep. No. 99-541, *supra*, 1986 U.S. Code Cong. & Admin. News, p. 3559.)

To serve both purposes, the statute takes the power to disclose user communications out of the hands of the provider except in narrow circumstances, none of which are even arguably met here. Because no pertinent textual exceptions apply, the SCA's disclosure prohibitions accordingly should be enforced according to their terms.

Nor should the Court should construe the SCA's prohibitions in a way that weakens them. Because the statutory text is clear and uncompromising, it could not reasonably bear a narrowing construction even if there were a sound reason to seek one. As explained below, however, there is no plausible basis to find the SCA unconstitutional as applied here, and thus there is no legitimate reason to construe it to permit the disclosures Real Parties seek.

II. THE SCA MAY BE CONSTITUTIONALLY APPLIED TO PROHIBIT PRETRIAL DISCLOSURES TO A CRIMINAL DEFENDANT.

Real parties concede that the SCA preempts any application of state law to require production of the information at issue here (RBM 4-5). They have no choice: because the SCA prohibits disclosure of the information real parties seek, any state law principle compelling disclosure would make "compliance with both state and federal law ... impossible." (*ONEOK v. Learjet, Inc.* (2015) 135 S.Ct. 1591, 1595 [191 L.Ed.2d 511].) California law "cannot be enforced in a way that compels [a service provider] to make disclosures violating the [SCA]." (*Negro*, 230 Cal.App.4th at 889.)

Because Congress's power to enact the prohibition is also unquestioned, a court could order production of the relevant records only if the statute is unconstitutional as applied or can be construed not to reach these materials. In assessing the balance between statutory command and constitutional prerogative, however, the Court should bear in mind that the SCA itself is designed to preserve Fourth Amendment interests as well as

broader privacy concerns. (See *Juror Number One*, supra, 206 Cal.App.4th at 860-61.) Weighed in that balance, Real Parties' strained constitutional claims cannot prevail. Rather than reiterate the detailed arguments in the answer brief on the merits, this brief focuses on the principles guiding resolution of the constitutional questions here.

To begin with, a criminal defendant does not have a constitutional right to compel production of any evidence he believes might assist his defense. Some information is simply out of reach. The Supreme Court has recognized a general "right to every man's evidence," but that right does not reach "persons protected by a ... statutory privilege." (*United States v. Nixon* (1974) 418 U.S. 683, 709 [94 S.Ct. 3090, 41 L.Ed.2d 1039].) Although a "generalized assertion of privilege must yield to the demonstrated, specific need for evidence in a pending criminal trial" (*id.* at 713), the SCA's prohibitions on disclosure produce a very specific privilege for providers: Providers are not merely excused from providing certain types of evidence, but are affirmatively forbidden to do so.

Criminal defendants face a steep burden in seeking to displace a federal privilege. (*E.g.*, *Miller*, supra, 21 Cal.4th at 901 [citing *Swidler & Berlin v. United States* (1998) 524 U.S. 399 [118 S.Ct. 2081, 141 L.Ed.2d 379]].) As Real Parties recognize, they can overcome the disclosure prohibitions of the SCA only by demonstrating a federal constitutional right to obtain the contested information from providers.

They cannot do so, for two principal reasons. First, Real Parties have no federal constitutional right to the information. Second, if they applied at all, the relevant constitutional principles would constrain the prosecuting authorities and courts, not private third parties like providers of electronic communications or remote computing services. Because the SCA permits prosecutors (on a proper showing) to obtain access to the contested information, and because they have a federal constitutional duty to provide

the defense with any exculpatory information they might obtain, prosecuting authorities—again, upon a proper showing by the defense—may properly be put to the choice of using their power to obtain the potentially exculpatory information or dismissing the prosecution.

A. Criminal defendants have no federal constitutional right to investigative tools that are equal or even similar to those available to law enforcement agencies.

Real Parties rest their constitutional arguments on false premises. Most striking is the notion that criminal defendants are entitled to the same scope of information and the same investigative tools that are available to law enforcement agencies and prosecuting authorities. Real Parties suggest that the U.S. Supreme Court’s decision in *Wardius v. Oregon* (1973) 412 U.S. 470, 474 [93 S.Ct. 2208, 37 L.Ed.2d 82], recognizes a symmetry principle of this kind. But *Wardius* does not sweep nearly so far. The Court did say that “discovery must be a two-way street” (*id.* at 475), but the Court was addressing only compelled *disclosure* by the defendant of “the details of his own case” (*id.* at 476) that was not counterbalanced by a symmetrical disclosure requirement for the prosecution. That is, if a state requires discovery *from* the defendant to the prosecution, the Court held that the state must require reciprocal discovery of the same scope *to* the defendant from the prosecution. But there is no general rule of parity, and the application of the SCA here is not unconstitutional merely because its exceptions reflect the government’s favored status.

On the contrary, while the Constitution tolerates a significant imbalance of investigative tools that favors law enforcement, other constitutional guarantees partly restore the balance. In particular, under *Brady v. Maryland* (1963) 373 U.S. 83, and subsequent decisions, a criminal defendant has a due process right to “evidence favorable to an accused” that is “material either to guilt or to punishment.” (*Id.* at 87.) The

prosecution's duty of disclosure under *Brady* has been expanded beyond the limits of the original decision, most notably to "encompass[] impeachment evidence as well as exculpatory evidence." (*United States v. Bagley* (1985) 473 U.S. 667, 676 [105 S.Ct. 3375, 87 L.Ed.2d 481].)

Thus, the actual constitutional balance of power does not require defendants to have the same investigative tools as the prosecution, but does ensure that defendants receive any exculpatory and impeachment evidence that the government finds using its superior investigative tools and powers. Conversely, while the government has an obligation to produce helpful information in its possession to the defense, the defense has no corresponding obligation to produce incriminating evidence to the prosecution, and indeed can rest on the Fifth Amendment protection against compelled self-incrimination. The powers and privileges on each side are complementary rather than congruent.

B. Criminal defendants have no constitutional right of access to third-party evidence before trial.

Real parties ask this Court to overrule *People v. Hammon* (1997) 15 Cal.4th 1117, and hold instead that criminal defendants are entitled to pretrial discovery of evidence from third parties. There is no basis to revisit the relevant holding of *Hammon*. This Court correctly concluded that neither Due Process nor any other federal constitutional protection requires pretrial discovery, and Real Parties do not identify any change in U.S. Supreme Court precedent that could support a different conclusion now.

Real parties tellingly fail to identify any decision of the U.S. Supreme Court holding that criminal defendants have a federal constitutional right to pretrial discovery. That is because the Court has repeatedly recognized that "there is no general constitutional right to discovery in a criminal case." (*Weatherford v. Bursey* (1977) 429 U.S. 545, 559 [97 S.Ct. 837, 51 L.Ed.2d 30]; see *People v. Valdez* (2012) 55 Cal.4th

82, 109-110.) Moreover, in *Wardius* the Court observed that “the Due Process Clause has little to say regarding the amount of discovery which the parties must be afforded” (412 U.S. at 474.) Indeed, a criminal defendant’s motion for discovery is not constitutionally based, but “is addressed solely to the sound discretion of the trial court, which has inherent power to order discovery when the interests of justice so demand.” (*Pitchess v. Superior Court* (1974) 11 Cal.3d 531, 535.)

Nor does the Confrontation Clause embrace a right to pretrial discovery that a defendant desires in order to optimize confrontation at trial. (See *Hammon*, 15 Cal.4th at 1125-28; *In re Crisis Connection, Inc.* (2011) 949 N.E.2d 789, 797 [following *Hammon*].) (Of course, the Confrontation Clause could not provide any basis for discovery of the account of a murder victim, who will never appear as a trial witness.)

Similarly, the right to compulsory process has never extended beyond process for trial, and Real Parties provide no basis to conclude otherwise. It also is well established—by the opinion of the Court in *Pennsylvania v. Ritchie*, not just the plurality opinion—that the right to “compulsory process provides no *greater* protections in this area than those afforded by due process.” (*Pennsylvania v. Ritchie* (1987) 480 U.S. 39, 56 [107 S.Ct. 989, 94 L.Ed.2d 40] [emphasis in original].) *Ritchie* itself, of course, involved information in the possession of the government, and thus subject to *Brady* disclosure. (See *id.* at 56-57.) Indeed, the *Brady* obligation was the basis for the Court’s holding. (See *ibid.*)

The nearest principle Real Parties identify to support their claim for recognition of a new federal constitutional right to pretrial discovery is “a criminal defendant’s right to have a meaningful opportunity to present a complete defense.” (*Holmes v. South Carolina* (2006) 547 U.S. 319, 331 [126 S.Ct. 1727, 164 L.Ed.2d 503].) But that is a trial right that requires

that a defendant have reasonably free rein to present evidence (see *ibid.*), not a right to gather evidence from any desired third-party source.

Nor is there merit to Real Parties' contention that the prevalence of plea bargaining should spawn a federal constitutional right to third-party discovery. To begin with, "there is no constitutional right to plea bargain" at all. (*Weatherford*, 429 U.S. at 561.) And even the prosecution's *Brady* duties do not reach the plea-bargaining stage: "the Constitution does not require the Government to disclose material impeachment evidence prior to entering a plea agreement with a criminal defendant." (*United States v. Ruiz* (2002) 536 U.S. 622, 632 [122 S.Ct. 2450, 153 L.Ed.2d 586].) That is because "impeachment information is special" only "in relation to the *fairness of a trial*, not in respect to whether a plea is *voluntary*." (*Id.* at 629 [emphasis in original].) Thus, while a defendant is entitled to counsel at the plea stage who effectively evaluates the law on the available facts (*e.g.*, *Lafler v. Cooper* (2012) 132 S.Ct. 1376 [182 L.Ed.2d 398]), there is no constitutional entitlement to access to all evidence that might bear on the strategy or ultimate result of plea bargaining.

III. PUBLIC POLICY FAVORS UPHOLDING AND ENFORCING THE SCA ACCORDING TO ITS TERMS.

A. Less restrictive means provide reasonable access to the information at issue.

Real Parties suggest that public policy requires weakening the protective disclosure prohibitions in the SCA, but overstate the burdens imposed on criminal defendants. Contrary to Real Parties' contentions, criminal defendants seeking to review the exculpatory contents of the social media account of a victim or witness have many options that provide access to the material without requiring any breach of the SCA. (See *O'Grady*, 139 Cal.App.4th at 1447 [SCA "does not render the data wholly

unavailable; it only means that the discovery must be directed to the owner of the data”].)

1. A user or recipient may authorize (or may be compelled to authorize) disclosure under the SCA.

Most obviously, a social media account-holder can be subpoenaed and compelled to produce material directly or consent to its disclosure. (See, e.g., *Negro*, 230 Cal.App.4th at 893, 895-899.) “[C]ourt-ordered consent” is “effective to satisfy the [SCA].” (*Id.* at 897 [citing *Romano v. Steelcase Inc.* (2010) 30 Misc.3d 426, 435, [907 N.Y.S.2d 650, 657]; *Al Noaimi v. Zaid* (D.Kan. 2012) 2012 WL 4758048; *In re Subpoena Duces Tecum to AOL, LLC* (E.D.Va. 2008) 550 F.Supp.2d 606, 613 n. 5; *Glazer v. Fireman’s Fund Ins. Co.* (S.D.N.Y. 2012) 2012 WL 1197167, at *3]; see also, e.g., *Flagg v. City of Detroit* (E.D.Mich. 2008) 252 F.R.D. 346, 363 [concluding, in civil discovery context, that “a party may be compelled to give its consent” to disclosure of text messages by service provider]; cf. *Bower v. Bower* (D.Mass. 2011) 808 F.Supp.2d 348, 350 [noting undisputed power in similar setting].)

And “coerced consent in such circumstances” is not “a novel idea.” (*Negro*, 230 Cal.App.4th at 897 [collecting cases].) Although this process is indirect, its circuitousness reflects the federal interests promoted by the SCA, i.e., protecting user privacy and limiting burdens on providers.

Where a defendant is aware of another person with access to the social media accounts of someone of interest, that person might consent (or, upon a showing to the court, might be required to consent) to disclosure of communications to which the account holder has granted her access as a “friend” or other member of a social circle. That certainly might happen when the defendant had friends or acquaintances in common with the victim or witness. (See *Ehling v. Monmouth-Ocean Hospital Service Corp.*(D.N.J. 2013) 961 F.Supp.2d 659, 669-71 [disclosure upon

authorization by account holder's Facebook friend complied with SCA].) Disclosure "with the lawful consent of ... an addressee or intended recipient of such communication" is permitted under the SCA (18 U.S.C. § 2702(b)(3)). Indeed, a "addressee or intended recipient" could comply with a personal subpoena by simply providing access to a series of postings or messages without any action by the provider.¹

2. A decedent's account may have a successor with authority to consent to disclosure under the SCA.

Despite Real Parties' dire depiction, it is not impossible for a criminal defendant to gain access to social media information even when an account holder is deceased. On the contrary, several options are available.

As in the situation where the account holder cannot be found or refuses to comply with a court order, an "addressee or intended recipient" could be subpoenaed to provide the information. In addition, although practices vary from user to user and provider to provider, the account may designate a person as a successor who can manage the account and who is susceptible to consent (or judicial compulsion to consent). For example, Google permits users to designate authorized successors through its Inactive Account Manager program. (See, e.g., <https://support.google.com/accounts/answer/3036546?hl=en>; <http://googlepublicpolicy.blogspot.com/2013/04/plan-your-digital-afterlife-with.html>.) Even when a deceased user has not taken advantage of the Inactive Account Manager, a surviving close family member may be able to obtain disclosure. (See <https://support.google.com/accounts/contact/deceased?hl=en>.) And because a criminal defendant is a "person other than a government agency," a

¹ That is what appears to have happened in *United States v. Pierce* (2d Cir. 2015) 785 F.3d 832, 842, where a defendant who was unable to enforce a subpoena seeking information from a Facebook account later reported to the court "that he had received the contents of the ... Account through the work of a private investigator."