Loyola of Los Angeles Law Review

Volume 55 | Number 3 Article 7

7-24-2022

# Social Media and the Stored Communications Act: Translating the Statutory Bar on Disclosure of Private Communications from Civil to Criminal Discovery

Michelle Korol

# SOCIAL MEDIA AND THE STORED COMMUNICATIONS ACT: TRANSLATING THE STATUTORY BAR ON DISCLOSURE OF PRIVATE COMMUNICATIONS FROM CIVIL TO CRIMINAL DISCOVERY

*Michelle Korol*∗

*The Stored Communications Act (SCA) is a federal statute that protects internet users from having their private online communications wrongfully disclosed by the providers that facilitate and store this information. Since 1986, courts have struggled to apply the proverbial "square peg" of the SCA's framework to the "round hole" of an ever-evolving internet world. The emergence of social media presented a new challenge for the courts. As of 2010, the SCA's protections have applied, in civil litigation, to information housed on various social media sites. But courts have only recently begun to grapple with the SCA's scope in relation to discovery in criminal prosecutions. In 2020, the California Supreme Court left open the question of whether a criminal defendant's constitutional rights permit that defendant to compel social media communications during his pretrial investigation where the SCA does not. This Note argues that a criminal defendant does not have a right—under the SCA, the Fifth and Sixth Amendments, or otherwise—to private, third-party social media communications in pretrial discovery. When the California Supreme Court litigates this issue, it should hold that the SCA's bar on a criminal defendant's ability to compel the disclosure of such communications from providers is not unconstitutional.*

∗ J.D. Candidate, 2022, LMU Loyola Law School, Los Angeles; B.A. Political Science, University of California, Los Angeles, March 2019. Thank you to Professor Kevin Lapp, whose thoughtful edits and feedback on this Note were invaluable. Thanks, also, to the *Loyola of Los Angeles Law Review* editors and staff for their hard work and tireless attention to detail. Lastly, thank you to my family and to the faculty at Loyola for fostering my curiosity and love of learning.

TABLE OF CONTENTS

## I. INTRODUCTION

In the last decade, technology giants have repeatedly come under fire, both for refusing to comply with requests for user information that could assist in criminal investigations, and conversely, for cooperating with law enforcement and releasing such information.[1] Datasets released by Twitter indicate that, in 2020, the provider honored 59.5 percent of law enforcement requests for user information within the United States.[2] Strikingly, Facebook's own metrics reveal that in that same year, it complied with 88.5 percent of government requests.[3] The information provided by Facebook can include GPS location data, billing records, associated phone numbers, user activity on the site, and the contents of private Messenger communications.[4]

Social media providers' business interests in protecting their users' privacy are often at odds with requests from the government to assist in ongoing investigations. Moreover, providers also routinely protect customers' private communications from the prying eyes of non-governmental entities. This tension is a function of a structure that positions the providers as the gatekeepers to our most intimate communications.

The Federal Stored Communications Act[5] (SCA), is at the core of this dynamic. The SCA protects internet subscribers from having their

1. *Compare* Thomas Brewster, *Apple Helps FBI Track Down George Floyd Protester Accused of Firebombing Cop Cars*, FORBES (Sept. 16, 2020, 10:15 AM), https://www.forbes.com/sites/thomasbrewster/2020/09/16/apple-helps-fbi-track-down-george-floyd-protester-accused-of-firebombing-cop-cars (describing Apple's "controversial" willingness to provide law enforcement with incriminating videos from the iCloud account of an individual suspected of firebombing police cars during the George Floyd protests; Apple previously denied the FBI's requests to break into the physical iPhones of the Saudi national who killed three people on the Pensacola, Florida, naval base), *with* David Ingram, *Zuckerberg's End-to-End Encryption Plan Could Put Facebook at Odds with Law Enforcement*, NBC NEWS (Mar. 8, 2019, 2:24 PM), https://www.nbcnews.com/tech/tech-news/zuckerberg-plan-could-put-facebook-collision-course-law-enforcement-n981246 [https://perma.cc/5UCL-7WVF] (discussing government pushback against Facebook's plans to 'go[] dark,' or utilize end-to-end encryption to put the contents of user communications out of law enforcement's reach).

2. *Transparency Report 17: January–June 2020—Information Requests (United States)*, TWITTER, https://transparency.twitter.com/en/reports/countries/us.html#2020-jan-jun [https://perma.cc/TD42-R29B]; *Transparency Report 18: July–December 2020—Information Requests (United States)*, TWITTER, https://transparency.twitter.com/en/reports/countries/us.html#2020-jul-dec [https://perma.cc/NLC8-8DED].

3. *Government Requests for User Data*, META, https://transparency.facebook.com/government-data-requests/country/US [https://perma.cc/79WH-NGJ7].

4. Ella Fassler, *Here's How Easy It Is for Cops to Get Your Facebook Data*, ONEZERO (June 16, 2020), https://onezero.medium.com/cops-are-increasingly-requesting-data-from-facebook-and-you-probably-wont-get-notified-if-they-5b7a2297df17 [https://perma.cc/AA5F-DHW5].

5. 18 U.S.C. §§ 2701–2713 (2018).

private electronic communications disclosed by the providers that facilitate and store this information.[6] As a baseline, the statute renders subpoenas to obtain electronic communications from providers unenforceable.[7] However, the SCA does outline a few, narrow exceptions to the general prohibition on disclosing the contents of communications.[8] Moreover, while the statute prescribes a general prohibition on disclosures of the contents of communications to non-governmental entities, it expressly authorizes the government to compel such disclosures where the governmental entity offers "specific and articulable facts" showing that the communications are "relevant and material to an ongoing criminal investigation."[9]

In both federal- and state-level civil litigation, courts have routinely applied the SCA to bar non-governmental entities from forcing social media providers to disclose their users' online communications.[10] But courts have only recently begun to grapple with the SCA's scope in relation to criminal prosecutions. Criminal prosecutions invoke a different set of considerations than civil litigation, including the defendant's constitutional right, under the Fifth and Sixth Amendments, to present a complete defense, which must be considered in light of the SCA's prohibitions on disclosure. Notably, the government can rely on various procedural mechanisms designated by the statute to obtain electronic communications.[11] Thus, the crux of the issue lies in defining the scope of a criminal defendant's right to directly access the same information.

In particular, the basic scenario explored in this Note arises when a criminal defendant seeks to obtain from a provider a victim's or key witness's social media communications—meaning posts, comments, or private messages—on the ground that this information potentially contains exculpatory evidence. The criminal defendant is a non-party to the communications, which are between the victim or witness and a third party. (If the defendant were the sender or the recipient, he would be legally entitled to obtain the archived communications from

6. Timothy G. Ackermann, *Consent and Discovery Under the Stored Communications Act*, FED. LAW., Nov.–Dec. 2009, at 42, 42, https://www.fedbar.org/wp-content/uploads/2009/11/storedcommunicationsact-pdf-1.pdf [https://perma.cc/C2T9-S545].

7. *Id.*

8. 18 U.S.C. § 2702(b).

9. *Id.* § 2703(d).

10. Ackermann, *supra* note 6, at 42.

11. 18 U.S.C. § 2703.

the provider.)[12] Citing the SCA, providers like Facebook routinely refuse such requests from defendants.[13] For example, in *Facebook, Inc. v. Superior Court of San Diego County* ("*Touchstone*"),[14] the defendant was charged with attempted murder and sought the victim's communications from before and after the shooting to support his claim of self-defense.[15] Facebook refused to comply with his subpoena for information, citing the SCA.[16] Such scenarios raise the question: does a defendant have a right—under the SCA, the Fifth and Sixth Amendments, or otherwise—to private, third-party social media communications to formulate a complete defense?

Faced with this issue in August 2020, the California Supreme Court decided that it would not rule on the constitutional questions raised by *Touchstone* and remanded the case to the lower court on other grounds.[17] Moreover, this decision came on the heels of a similar denial from earlier that year, in which the United States Supreme Court declined to take up a case concerning two criminal defendants' rights to obtain user communications from Facebook.[18]

Courts cannot ignore the constitutional issue indefinitely. This Note argues that when the California Supreme Court does ultimately take up the issue, it should rule that the SCA's bar on a criminal defendant's ability to compel the disclosure of private, third-party communications from providers is not unconstitutional.

To that end, Part II will outline the basic structure of the SCA to explain the dichotomy that allows the government to obtain social media communications, while prohibiting the defendant from doing the same. Next, Part III will briefly examine how courts have applied the SCA to social media information in civil litigation to contextualize further discussion. Part IV will analyze the SCA in relation to criminal defendants' pretrial requests for disclosures of social media communications through a statutory, constitutional, and policy-oriented perspective. On the statutory level, this discussion will demonstrate that

12. *See* 18 U.S.C. § 2702(b)(1) (a provider may divulge the contents of a communication "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient").

13. Gilad Edelman, *Facebook and Twitter Want to Keep the Justice System Stacked Against Defendants*, WIRED (June 19, 2020, 7:00 AM), https://www.wired.com/story/facebook-twitter-criminal-justice-stored-communications-act/ [https://perma.cc/PKQ3-HH78].

14. 471 P.3d 383 (Cal. 2020).

15. *Id.* at 387.

16. *Id.* at 387, 390.

17. *Id.* at 402–03.

18. Facebook, Inc. v. Superior Ct., 140 S. Ct. 2761, 2761 (2020).

the SCA facially prohibits providers from complying with criminal defendants' subpoenas for private, third-party communications, which do not squarely fall under any of the enumerated exceptions. Next, this discussion will introduce the constitutional issues implicated by the SCA's statutory bar and the question yet to be resolved by the California Supreme Court: whether the SCA is unconstitutional as applied in criminal prosecutions. Ultimately, this Note will argue that California courts and courts in various other jurisdictions are correct in unanimously holding that criminal defendants do not have an affirmative, constitutional right to private, third-party communications in pretrial discovery.[19] Finally, this discussion will assess the policy implications of broadening the SCA's scope in criminal prosecutions and advocate against such a significant intrusion on privacy and victims' rights. Part V will conclude.

## II. UNDERSTANDING THE SCA

The SCA is the lifeblood of privacy for internet communications in the United States. It was enacted in 1986 as Title II of the Electronic Communications Privacy Act.[20] In enacting this legislation, Congress's purpose was "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs."[21] Procedurally, the SCA comes into play when a party to litigation, or the government, seeks to compel information from a non-party internet service provider (ISP).[22]

Under the third-party doctrine, the United States Supreme Court has routinely held that the Fourth Amendment does not protect information revealed to third parties.[23] Thus, while the Fourth Amendment generally provides privacy protections for our homes and their contents,[24] it may not, alone, offer privacy protections for our internet

19. People v. Webb, 862 P.2d 779, 794 (Cal. 1993) (the California Supreme Court has repeatedly declined to recognize a Sixth Amendment right to defense pretrial discovery of otherwise privileged or confidential information).

20. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 1848.

21. S. REP. NO. 99-541, at 3 (1986).

22. Rudolph J. Burshnic, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 WASH. & LEE L. REV. 1259, 1275 (2012) (explaining that parties to a case are subject to discovery procedures, while non-parties can be compelled to produce information by order of a subpoena).

23. *See* United States v. Miller, 425 U.S. 435, 443 (1976); Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

24. *See* Kyllo v. United States, 533 U.S. 27, 31 (2001).

communications, which do not exist in our "home."[25] Rather, we "share" these communications with private third parties, who store them on remote network servers.[26] Accordingly, there is some debate as to whether internet users may claim any "reasonable expectation of privacy" in such information.[27]

The privacy debate also factors in the nature of the electronic information. Internet users produce two types of information: (1) content information, meaning "any information concerning the substance, purport, or meaning of that communication"[28]—or in layman's terms, a "communication"; and (2) non-content records, a blanket term encompassing all other electronic information, (including a subcategory referred to as "basic subscriber information," which involves information about the subscriber's identity).[29] For example, the body of a private message sent on Facebook Messenger would constitute content information. In contrast, a log that includes a list of recipients of such private messages and the dates and times of such communications, among other things, would constitute non-content information. Courts have already explicitly held that an internet user does not have a constitutionally derived expectation of privacy in *non-content* information shared with ISPs.[30] Whether the *contents* of our internet communications invoke Fourth Amendment protections remains a constitutional gray area.[31]

The legislature enacted the SCA to fill the privacy gap by "creat[ing] a set of Fourth Amendment-like privacy protections by statute."[32] The SCA governs ISPs, prohibiting them from disclosing the information they facilitate and store on our behalf to both governmental and non-governmental entities unless the enumerated

25. Juror No. One v. Superior Ct., 142 Cal. Rptr. 3d 151, 155 (Ct. App. 2012); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209–10 (2004).

26. S. REP. NO. 99-541, at 3 (1986) (noting that because electronic files are "subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection" absent legislation); Kerr, *supra* note 25, at 1209–10.

27. Kerr, *supra* note 25, at 1210–11.

28. 18 U.S.C. § 2510(8) (2018); *see id.* § 2711(1) (providing that the operative definitions for some of the terms used in the SCA can be found in section 2510 of the Wiretap Act).

29. Kerr, *supra* note 25, at 1219.

30. *Id.* at 1210 (citing Guest v. Leis, 255 F.3d 325, 335–36 (6th Cir. 2001) (finding no reasonable expectation of privacy in non-content information shared with ISPs); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (same); United States v. Hambrick, 55 F. Supp. 2d 504, 508–09 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000) (same)).

31. Kerr, *supra* note 25, at 1210–11.

32. *Id.* at 1212.

conditions are met.[33] These protections shield content and non-content information from the government by limiting when the government can compel information from ISPs.[34] The SCA also restricts what ISPs can otherwise voluntarily disclose to non-governmental parties, such as marketers and private litigants.[35] Notably, this structure provides no mechanism for criminal defendants to obtain the *contents* of third-party communications.

It is also important to note that the SCA's protections only apply when the information sought is not "readily accessible to the general public."[36] The SCA does not apply to electronic communications that are configured to be publicly available.[37] For example, the contents of a public post on a Facebook user's "wall" would not be treated the same as the body of a private message.

### *A. Entities Governed by the SCA*

The SCA applies to two kinds of ISPs: those that give users the ability to send or receive electronic communications, Electronic Communications Services (ECS), and those that provide computer storage and processing services, Remote Computing Services (RCS).[38] The language of the statute, which is outdated in its conception of the internet, treats these two functions as separate.[39] However, Congress did contemplate that ECS providers could also provide some form of storage, whether for "purposes of backup," or the "temporary, intermediate" storage required to transmit the communication.[40] Today, many ISPs perform both functions.[41] Thus, in modern-day applications, "[t]he classifications of ECS and RCS are context sensitive: the key is the provider's role with respect to a particular copy of a particular communication."[42] By extension, if an entity is neither an ECS nor

33. *Id.* at 1212–13.
34. *Id.*
35. *Id.* at 1213.
36. 18 U.S.C. § 2511(g)(i) (2018).
37. *Id.*
38. Kerr, *supra* note 25, at 1214.
39. *See* 18 U.S.C. § 2703; Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (noting that "Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results").
40. 18 U.S.C. § 2510(17).
41. Kerr, *supra* note 25, at 1215.
42. *Id.*

RCS provider with respect to a certain communication, then the SCA does not apply; instead, only Fourth Amendment protections apply.[43]

The classifications themselves are not determinative of the central premise of this Note, which is that the SCA does not permit criminal defendants to compel a provider to disclose the *contents* of private, third-party communications, regardless of the service it provided with respect to that communication. Nor do criminal defendants have a constitutional right to those communications in either circumstance.[44] For purposes of this Note, the classifications are relevant to the extent that they determine whether the social media provider falls into either one of those categories, and thus, is subject to the SCA's prohibitions on disclosure. Moreover, defining these classifications is crucial to understanding the spectrum of procedural mechanisms for compelled disclosure that are exclusively available to the government and how they are satisfied, as well as the requirements providers must comply with to disclose communications.[45]

Sections II.B and C outline the SCA's framework for disclosures of information facilitated and stored by ISPs. Table 1 (below) provides additional context by synthesizing the basic structure of the SCA's disclosure requirements, ordered from most to least protected type of electronic information.

43. Burshnic, *supra* note 22, at 1282.

44. *See infra* Section IV.B.

45. *See* 18 U.S.C. § 2703(c)(2), (d) (2018) (dictating procedures for the government to compel disclosure of electronic communications); *id.* § 2702 (outlining nine exceptions under which providers may voluntarily disclose the contents of communications).

**Table 1:** Basic Structure of the SCA's Disclosure Requirements[46]

| | Voluntary Disclosure [§ 2702] | | Compelled Disclosure [§ 2703] | |
|---|---|---|---|---|
| Type of Electronic Information | Governmental Entities? | Non-Governmental Entities? | Governmental Entities? | Non-Governmental Entities? |
| Communications stored for < 180 days | No—unless a § 2702(b) exception applies [§ 2702(a)(1)–(2)] | No—unless a § 2702(b) exception applies [§ 2702(a)(1)–(2)] | Yes—by search warrant [§ 2703(a)] | No—unless a § 2702(b) exception applies [§ 2702(a)(1)–(2)] |
| Communications stored for > 180 days | No—unless a § 2702(b) exception applies [§ 2702(a)(1)–(2)] | No—unless a § 2702(b) exception applies [§ 2702(a)(1)–(2)] | Yes—by search warrant [§ 2703(a)]; by subpoena (with notice) or court order (with notice) [§ 2703(d)] | No—unless a § 2702(b) exception applies [§ 2702(a)(1)–(2)] |
| Non-content records | No—unless a § 2702(b) exception applies [§ 2702(a)(3)] | Yes [§ 2702(c)(6)] | Yes—by search warrant [§ 2703(c)(1)]; by court order [§ 2703(d)] | See instead—voluntary disclosure [§ 2702(c)(6)] |
| Basic subscriber information | No—unless a § 2702(b) exception applies [§ 2702(a)(3)] | Yes [§ 2702(c)(6)] | Yes—by search warrant [§ 2703(c)(2)]; by subpoena or court order [§ 2703(d)] | See instead—voluntary disclosure [§ 2702(c)(6)] |

### *B. Compelled Disclosure to the Government—18 U.S.C. § 2703*

Section 2703 dictates a scheme of procedural standards the government must satisfy to compel different types of communications. For example, to compel a provider of ECS to disclose the contents of communications that it possesses and stores for 180 days or less, the government must obtain a search warrant.[47] If the ECS provider has stored the contents for greater than 180 days, or the government seeks to compel a provider of RCS to disclose contents, the government may do so in a couple of ways.[48] The government can obtain a search warrant.[49] Alternatively, the government can use a subpoena or a court order pursuant to section 2703(d), so long as this process is combined

46. *See infra* Sections II.B–C.
47. 18 U.S.C. § 2703(a).
48. *Id.* § 2703(a)–(b).
49. *Id.* § 2703(b)(1)(A).

with prior notice to the subscriber or customer.[50] To obtain the court order, the government must provide "specific and articulable facts showing that there are reasonable grounds to believe" that the communication and the related information sought are "relevant and material to an ongoing criminal investigation."[51] In other words, the government faces a higher barrier to access for more recent communications, and historic communications are marginally easier to obtain.

Thus, if law enforcement is seeking disclosure of an individual's Facebook Messenger communications from within the last 180 days, for example, the government must obtain a search warrant.[52] However, where the private messages sought are more than 180 days old, the government may either obtain a search warrant, or pursue a subpoena or section 2703(d) order and provide notice to the account holder. As an anecdotal example, a criminal complaint filed by the government within two weeks of the Capitol Hill Riot on January 6, 2021, revealed that in response to a search warrant, Facebook provided the FBI with the private messages and other associated information of an individual charged with storming the Capitol.[53]

It is important to note that the same rules governing compelled disclosure to the government also apply to non-content records, such as logs maintained by a network server.[54] This category can include information such as addresses of websites visited by the user, records of online settings and passwords, and email addresses of other users with whom the account holder has communicated.[55] To obtain such information, the government must undertake the same procedures of obtaining a search warrant, subpoena, or court order.[56]

The SCA provides an exception for compelling a narrow subset of non-content records known as "basic subscriber information."[57]

50. *Id.* § 2703(b)(1)(B), (d); *id.* § 2705.

51. *Id.* § 2703(d).

52. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010) (finding that Facebook is an ECS provider with respect to its private messaging function).

53. Complaint at 1, United States v. Kelly, No. 21-mj-00128 (D.D.C. Jan. 20, 2021); Thomas Brewster, *Facebook Gives FBI Private Messages of Users Discussing Capitol Hill Riot*, FORBES (Jan. 21, 2021, 5:59 AM), https://www.forbes.com/sites/thomasbrewster/2021/01/21/facebook-gives-fbi-private-messages-of-users-discussing-capitol-hill-riot/.

54. Kerr, *supra* note 25, at 1219.

55. Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 582 (2007).

56. 18 U.S.C. § 2703(c)(1)(A)–(C).

57. Kerr, *supra* note 25, at 1219.

The boundaries of this category of information are explicitly delineated in the statute.[58] These types of records include basic information about the subscriber's identity, such as a subscriber's name, address, number, local and long distance telephone records, duration of service and types of service utilized, and the means and source of payment for the service.[59] The legislature deemed this type of information to be less private than other non-content records and user communications.[60] Thus, if the government is seeking an individual's basic subscriber information from Facebook, the bar is lower than it would be for the Messenger communications. The government can obtain these records with a mere subpoena, meaning without obtaining a search warrant or the added requirement of providing notice to the consumer.[61] In sum, the SCA contains procedural mechanisms by which the government can obtain communications, non-content records, and basic subscriber information from ISPs.

### *C. Voluntary Disclosure by the Provider—18 U.S.C. § 2702*

On the other side of the coin, section 2702 of the SCA governs voluntary disclosures by ECS and RCS providers that provide services "to the public."[62] The statute permits such providers to voluntarily disclose non-content records, including basic subscriber information, to non-governmental entities, such as marketing companies and other private parties.[63] In contrast, as previously discussed, the SCA only permits providers to disclose this type of user information to the government pursuant to a search warrant, subpoena, or court order.[64]

Communications are treated differently. Section 2702 generally bars providers from voluntarily disclosing the *contents* of communications.[65] However, the statute also lists nine specific circumstances that qualify as exceptions to this general rule.[66] As discussed at greater length below,[67] a criminal defendant seeking to obtain private, third-party communications—meaning communications of which he was

58. 18 U.S.C. § 2703(c)(2)(A)–(F).
59. *Id.*
60. *See id.*
61. *Id.* § 2703(c)(2).
62. 18 U.S.C. § 2702.
63. *Id.* § 2702(c)(6); Kerr, *supra* note 25, at 1220.
64. 18 U.S.C. § 2703(c)(1)–(2).
65. 18 U.S.C. § 2702(a).
66. *Id.* § 2702(b).
67. *See infra* Section IV.A.

neither the sender nor the intended recipient—for his defense will not fall under any of these enumerated exceptions. The exceptions do not permit disclosure of communications to a criminal defendant unless the defendant was either the sender or the intended recipient,[68] or there is lawful consent to the disclosure by the sender or intended recipient.[69]

## III. THE SCA IN CIVIL LITIGATION

This part explains when and how courts have interpreted the SCA to allow or prohibit a provider to disclose social media communications. Civil litigation in both the federal and state courts reveals that the SCA applies to various social media platforms and generally prohibits non-governmental entities from compelling disclosure of the contents of communications.[70] The body of case law involving the SCA's application is more extensive in civil litigation than in criminal prosecutions. Thus, in construing how the SCA applies to criminal defendants, courts tend to anchor their analyses to civil precedent.[71] The civil cases reveal that the SCA's prohibitions on disclosure to non-governmental entities can apply to email services,[72] text-messaging services,[73] voicemail services,[74] and video-sharing services.[75] In 2010, the Central District of California established that the SCA also extends to social networking sites, protecting communications on those platforms from disclosure as well.[76]

68. 18 U.S.C. § 2702(b)(1).

69. 18 U.S.C. § 2702(b)(3) is often referred to as the "lawful consent exception." *See, e.g.*, Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 738 (Cal. 2018).

70. Ackermann, *supra* note 6, at 42.

71. *See, e.g.*, *Hunter*, 417 P.3d at 741.

72. Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004); *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008).

73. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902–03 (9th Cir. 2008).

74. State Wide Photocopy Corp. v. Tokai Fin. Servs., Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995); *see* United States v. Steiger, 318 F.3d 1039, 1048 (11th Cir. 2003) (citing Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002)); United States v. Councilman, 418 F.3d 67, 78–79 (1st Cir. 2005) (en banc).

75. Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008); Ackermann, *supra* note 6, at 43.

76. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010). *See generally* 18 U.S.C. § 2702(a) (2018) (ECS and RCS providers are prohibited from voluntarily disclosing the contents of communications, barring an applicable statutory exception); *supra* Section II.C.

### *A. Case Study:* Crispin v. Christian Audigier, Inc.

The SCA was enacted prior to the emergence of social media as we know it. Thus, the statute does not contemplate whether social media platforms are ECS or RCS and subject to the SCA's protections. With the evolution of the internet and the growth of social media as a primary mode of online communication, it was only a matter of time before a court would be tasked with evaluating the SCA's applicability in this context. *Crispin v. Christian Audigier, Inc.*[77] is a landmark case in this respect, representing the first time a court interpreted the SCA's application to social networking sites.[78]

In *Crispin*, the plaintiff, an artist, filed an action against Christian Audigier, Christian Audigier, Inc., and their various sublicensees, alleging that the defendants had breached an oral agreement to use his artwork in a specified, limited manner for the Ed Hardy clothing brand.[79] The defendants served a subpoena on three social media sites, Facebook, Media Temple, and Myspace, seeking to compel them to disclose Crispin's basic subscriber information, communications between Crispin and a tattoo artist named Bryan Callan, and all communications that referred or related to Audigier, Christian Audigier, Inc., the Ed Hardy brand, or any of the other defendants.[80] Crispin filed a motion to quash the subpoena, arguing in part that the defendants sought electronic communications that the SCA prohibits ISPs from disclosing.[81]

As a threshold matter, the court considered whether Crispin could assert the rights of Facebook, Media Temple, and Myspace, none of which had moved to quash the subpoenas.[82] The court held that, while a party generally cannot object to a subpoena issued to a non-party, an individual has a personal right in information tied to his profile and inbox on a social networking site, and this right is sufficient to confer standing to move to quash a subpoena seeking such information.[83]

Next, the court evaluated how the SCA substantively applies to social networking sites. Initially, the court needed to determine whether Facebook, Media Temple, and Myspace fell into the ECS or

77. 717 F. Supp. 2d 965 (C.D. Cal. 2010).
78. *Id.* at 977; *see* Burshnic, *supra* note 22, at 1264.
79. *Crispin*, 717 F. Supp. 2d at 968.
80. *Id.* at 968–69.
81. *Id.* at 969.
82. *Id.* at 973.
83. *Id.* at 974.

RCS categories subject to the statute's protections.[84] Pulling from precedent concerning email service providers, the court found that these three entities also fell into the ECS category with respect to their private messaging functions.[85] However, the court further held that with respect to the *opened* private messages retained by the providers, those entities were also RCS providers.[86] Thus, the court found that both the opened and unopened communications on those sites were protected by the SCA and quashed the subpoenas.[87]

The court then considered whether the SCA applies to wall postings and comments on Facebook and Myspace.[88] In finding that those sites are ECS as to wall postings and comments, the court relied on precedent pertaining to electronic bulletin board systems (the dial-up equivalent to modern day internet message boards).[89] As with the bulletin board systems, the court reasoned, "the passive action of failing to delete" a Facebook or Myspace wall posting or comment "results in that post being stored for backup purposes."[90] The court noted that Congress contemplated this type of storage within the statute's definition of ECS providers.[91]

Acknowledging that this was a "difficult question," the court alternatively held Facebook and Myspace to be RCS providers with respect to wall postings and comments.[92] The court analogized Facebook and Myspace to YouTube, which had already been established as an RCS provider in *Viacom International, Inc. v. YouTube*.[93] In that case, the court categorized YouTube as an RCS provider subject to SCA protections because the site stores video "for the benefit of the user and those the user designates."[94]

84. *Id.* at 977–80.

85. *Id.* (citing Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900 (9th Cir. 2008) (finding that a pager text-messaging service was an ECS provider because it "enabled the plaintiff and others to 'send or receive . . . electronic communications'" (omission in original))).

86. *Id.* at 987.

87. *Id.*

88. *Id.* at 988–89.

89. *Id.*; *see also* Benj Edwards, *The Lost Civilization of Dial-Up Bulletin Board Systems*, THE ATLANTIC (Nov. 4, 2016), https://www.theatlantic.com/technology/archive/2016/11/the-lost-civilization-of-dial-up-bulletin-board-systems/506465/ [https://perma.cc/EDZ4-9TKK] (describing bulletin board systems).

90. *Crispin*, 717 F. Supp. 2d at 989.

91. *Id.* at 979; *see* 18 U.S.C. § 2510(17)(B) (2018).

92. *Crispin*, 717 F. Supp. 2d at 988–90.

93. *Id.* at 990; 253 F.R.D. 256 (S.D.N.Y. 2008).

94. *Crispin*, 717 F. Supp. 2d at 990 (discussing *Viacom Int'l*, 253 F.R.D. at 265).

Ultimately, after establishing these parameters for applying the SCA to social networking sites, the court remanded the case for additional findings of fact.[95] Most pertinently, the court found that the SCA expressly protects private messages on social media platforms.[96] However, the court directed that whether the wall postings and comments could be subpoenaed under the SCA hinged on whether the user had employed the privacy settings available through Facebook and Myspace to restrict that content from the general public.[97] If the social media user had employed a site's privacy settings to restrict the public's access to the user's content, the SCA would prohibit disclosure. In remanding the case, the court emphasized that "a review of plaintiff's privacy settings would definitively settle the question."[98]

### *B. Takeaways from* Crispin

According to *Crispin,* it is now evident that the SCA applies to various kinds of user information associated with social networking sites. With regard to disclosure, the *Crispin* court added an additional consideration into the mix: a user's privacy configurations on a given social media platform can be the determining factor in whether the SCA's protections apply to certain types of information. On the other hand, *Crispin* established that, as with emails, an account holder's communications via a social media platform's private-messaging function are firmly within the scope of the SCA's protections. This decision demonstrates that the SCA is available in civil litigation as a mechanism by which parties can prevent information associated with social media accounts from being disclosed by providers.

## IV. APPLYING THE SCA IN CRIMINAL PROSECUTIONS

The following discussion explores the SCA's contours in relation to criminal defendants' pretrial requests for disclosures of social media communications. As a baseline, a plain-language interpretation of the SCA indicates that the statute applies similarly in criminal prosecutions as it does in civil litigation. Next, this discussion will highlight the gray area that the California Supreme Court has thus far failed to resolve: whether a criminal defendant's constitutional rights permit

95. *Id.* at 991.
96. *Id.* at 981–82.
97. *Id.* at 991.
98. *Id.*

that defendant to compel social media communications during his pretrial investigation where the SCA does not.

To that end, the relevant analysis breaks down as follows. First, the SCA applies as a statutory bar against disclosure to criminal defendants who, in pretrial discovery, seek to subpoena social media information from providers in criminal prosecutions.[99] Second, California courts have correctly applied precedent in determining that criminal defendants do not have an overriding constitutional right to compel private, third-party communications in pretrial discovery.[100] Finally, a forward-looking analysis of the implications of allowing a non-party to private communications to obtain such information dictates that the privacy interests ensured by the SCA are incompatible with the creation of such an exception.[101]

### *A. Statutory Analysis: The SCA Facially Bars Providers from Disclosing Private Communications in Response to a Criminal Defendant's Subpoena*

Congress structured the SCA's rules governing disclosure of communications in three main parts. Subsection 2702(a) generally prohibits providers from "knowingly divulg[ing] to any person or entity the contents" of covered communications.[102] Subsection 2702(b) contains enumerated exceptions to this blanket prohibition.[103] Section 2703 sets out provisions under which governmental entities may compel disclosure from providers.[104] Notably, Congress did not include in this framework an exception for criminal defendants' subpoenas.

#### i. Structure and Legislative Intent

The California Supreme Court grappled with the SCA's scope in relation to a criminal defendant's request for third-party social media communications in two cases: *Facebook, Inc. v. Superior Court* ("*Hunter*")[105] and *Facebook, Inc. v. Superior Court of San Diego County* ("*Touchstone*").[106] In *Hunter*, the court addressed whether in criminal matters, "section 2702 bars covered service providers from

99. *See infra* Section IV.A.
100. *See infra* Section IV.B.
101. *See infra* Section IV.C.
102. 18 U.S.C. § 2702(a) (2018).
103. *Id.* § 2702(b).
104. 18 U.S.C. § 2703.
105. 417 P.3d 725, 727–28 (Cal. 2018).
106. 471 P.3d 383, 386 (Cal. 2020).

*divulging social media communications* in response to a subpoena."[107] Relying on civil litigation that previously addressed this same issue—namely the *Crispin* case—the court found that, as a baseline in criminal cases, "by virtue of section 2702(a) [governing voluntary disclosures], the [SCA] generally and initially prohibits the disclosure of *all* (even public) communications."[108]

Every other court to consider the issue has similarly found that a plain-language reading of the SCA facially bars providers from disclosing communications in response to a criminal defendant's subpoena.[109] For example, in *Facebook, Inc. v. Wint*,[110] the District of Columbia Court of Appeals explained that, "[r]ead together, §§ 2702 and 2703 appear to comprehensively address the circumstances in which providers may disclose covered communications. Those circumstances do not include complying with criminal defendants' subpoenas."[111] The Second Circuit reached a similar conclusion, finding that "[t]he SCA does not, on its face, permit a [criminal] defendant to obtain such information."[112] While the statute repeatedly references disclosures in response to subpoenas and other court orders, Congress notably stopped short of including an exception for criminal defendants' subpoenas.[113] Courts generally refuse to infer an exception into

107. *Hunter*, 417 P.3d at 741.

108. *Id.* at 741–44 (discussing *Viacom Int'l Inc. v. Youtube Inc*., 253 F.R.D. 256 (S.D.N.Y. 2008) and *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010)) ("Two additional section 2702 disclosure cases are more pertinent to our present inquiry because they concerned disclosure by service providers, not of private e-mail, but of *social media communications*.").

109. Facebook, Inc. v. Wint, 199 A.3d 625, 629 (D.C. 2019); *see also* State v. Bray, 422 P.3d 250, 256 (Or. 2018) ("A person like defendant, who is a nongovernmental entity, cannot require a remote computing service . . . to divulge the contents of communications."); State v. Johnson, 538 S.W.3d 32, 70 (Tenn. Crim. App. 2017) (holding "defendants cannot obtain . . . witnesses' electronic communications directly from the social media providers" under the SCA"); United States v. Nix, 251 F. Supp. 3d 555, 559 (W.D.N.Y. 2017) (the SCA "does not permit a defendant in a criminal case to subpoena the content of a Facebook or Instagram account"); United States v. Wenk, 319 F. Supp. 3d 828, 829 (E.D. Va. 2017) ("[T]he [SCA] does not contain a provision detailing the methods with which criminal defendants can *require* disclosure . . . .").

110. 199 A.3d 625 (D.C. 2019).

111. *Id.* at 628.

112. *Id.* at 629 (alteration in original) (quoting United States v. Pierce, 785 F.3d 832, 842 (2d Cir. 2015)).

113. *See, e.g.*, 18 U.S.C. § 2703(b)(1)(B), (c)(1)(A), (c)(2), (d), (e), (h)(2); *see also* Encino Motorcars, LLC v. Navarro, 138 S. Ct. 1134, 1143 (2018) ("[S]ilence in the legislative history, 'no matter how "clanging,"' cannot defeat the better reading of the text and statutory context.").

a statute where that statute otherwise specifically enumerates certain exceptions.[114]

Moreover, the legislative history of the statute highlights Congress's intent to limit "exceptions to the general rule of nondisclosure" to three categories: (1) disclosures that are authorized by either the sender or receiver of the message; (2) disclosures that are "necessary for the efficient operation of the communications system"; and (3) disclosures to the government.[115] This narrow range of exceptions reflects Congress's focus on achieving "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."[116] Thus, read together, the structure of the SCA and the accompanying legislative history provide strong support for the conclusion that the SCA prohibits providers from disclosing covered communications in response to criminal defendants' subpoenas.

### ii. The "Public/Private Configuration Distinction" as a Proxy Exception

In addressing the avenues of discovery still available to a criminal defendant in light of the SCA, the California Supreme Court drew a line between communications that are configured to be publicly accessible, and those which are configured as private or restricted.[117] The court concluded that, although the SCA initially bars the disclosure of *all* communications, the statute's "lawful consent exception [section 2702 (b)(3)] allows providers to disclose communications configured by the user to be *public*."[118] Here, the court turned to legislative intent, explaining that "[t]he legislative history suggests that Congress intended to exclude from the scope of the lawful consent exception communications configured by the user to be accessible to only specified

114. *See generally* United States v. Johnson, 529 U.S. 53, 58 (2000) ("When Congress provides exceptions in a statute, it does not follow that courts have authority to create others. The proper inference, and the one we adopt here, is that Congress considered the issue of exceptions and, in the end, limited the statute to the ones set forth."); O'Grady v. Superior Ct., 44 Cal. Rptr. 3d 72, 86 (Ct. App. 2006) (declining to infer civil-subpoena exception to SCA's nondisclosure provision because "[f]ew cases have provided a more appropriate occasion to apply the maxim *expressio unius exclusio alterius est*, under which the enumeration of things to which a statute applies is presumed to exclude things not mentioned").

115. S. REP. NO. 99-541, at 37–38 (1986).

116. H.R. REP. NO. 99-647, at 19 (1986).

117. Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 743–44 (Cal. 2018).

118. *Id.* at 741–44 (discussing Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010)) (emphasis added) ("[A]lthough we agree with the result in *Crispin*, we conclude that the decision in that case should have been grounded on the lawful consent exception to the general prohibition.").

recipients."[119] On the other hand, Congress stressed that when users post or communicate publicly, and/or accept a provider's terms of service, this constitutes implied lawful consent sufficient to permit disclosure by service providers.[120]

In practice, the "public/private configuration distinction" functions much like any other exception to the general statutory bar on disclosure. Publicly configured social media communications are considered "fair game" for a criminal defendant, meaning that the provider of that social media service cannot assert the SCA as grounds for refusing a defendant's subpoena to compel disclosure of such communications.[121] This does not affect the prohibition on compelling disclosure of, say, private messages exchanged via the Facebook Messenger platform. However, this does mean that whether a defendant can subpoena Facebook to compel disclosure of a Facebook user's posts or comments will depend on how that user configured the privacy settings for each individual communication.

Thus, the "public/private configuration distinction" narrows the relevant inquiry to whether a defendant can somehow obtain *private* communications despite the SCA's bar on disclosure. Given that the SCA is a dead end for a defendant who seeks private, third-party communications, criminal defendants who seek to gather such evidence to build their defense have turned to constitutional arguments.

### *B. Constitutional Analysis: Criminal Defendants Do Not Have an Overriding Constitutional Right to Disclosures of Private Communications*

In both *Hunter* and *Touchstone*, the defendants raised Fifth and Sixth Amendment claims, arguing that their federal constitutional rights to a fair trial, to present a complete defense, and to cross-examine witnesses supported their subpoenas.[122] Thus, they contended that the SCA is unconstitutional insofar as it affords providers a basis to refuse to comply with subpoenas from criminal defendants.[123] However, in both cases, the California Supreme Court failed to reach this

119. *Id.* at 747.

120. *See id.* at 739–40 (discussing H.R. REP. NO. 99-647 (1986)).

121. *See id.* at 750–51 (upholding the ruling in Negro v. Superior Ct., 179 Cal. Rptr. 3d 215, 234 (Ct. App. 2014) that "[i]nsofar as the Act permits a given disclosure, it permits a court to compel that disclosure under state law").

122. *Id.* at 732; Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383, 387 (Cal. 2020).

123. *Hunter*, 417 P.3d at 732; *Touchstone*, 471 P.3d at 387.

analysis, leaving the constitutional issues raised by the defendants unanswered.[124]

i. There Is No California Supreme Court Precedent on This Issue

In *Hunter*, the "public/private configuration distinction" proved to be a doctrinal safety net that prevented the California Supreme Court from resolving the attendant constitutional claims. Instead, the court cited well-established precedent, which holds that courts "should address and resolve statutory issues prior to, and if possible, instead of constitutional questions."[125]

Defendants Derrick Hunter and Lee Sullivan were indicted by a grand jury on murder, weapons, and gang-related charges arising out of a drive-by shooting in San Francisco.[126] Social media featured prominently in the case. At the grand jury proceeding, the prosecution's main theory of the case was that the shooters killed the victim, a member of a rival gang, because he had threatened Hunter's younger brother on social media.[127]

Both defendants served subpoenas on Twitter, seeking "'[a]ny and all public and private content' that had been 'published by'" Sullivan's once-girlfriend, the witness who had identified the defendants.[128] Sullivan also served similar subpoenas on Facebook and Instagram, requesting information published by the same key witness and the victim.[129] Relying on subsection 2702(a), Facebook, Instagram, and Twitter uniformly moved to quash the subpoenas, asserting that they were precluded by the SCA from disclosing the requested information.[130]

The defendants opposed the motions to quash.[131] They asserted their need for the victim's communications to challenge anticipated expert testimony that the shooting was gang-related, and to establish self-defense based on the victim's public posts showing that he had previously threatened the defendants and others on social media.[132]

124. *Hunter*, 417 P.3d at 745; *Touchstone*, 471 P.3d at 402.

125. *Hunter*, 417 P.3d at 745 n.31 (citing Santa Clara Cty. Loc. Transp. Auth. v. Guardino, 902 P.2d 225 (Cal. 1995); People v. Williams, 547 P.2d 1000 (Cal. 1976); and cases cited within).

126. *Hunter*, 417 P.3d at 729–30.

127. *Id.* at 730.

128. *Id.* (alteration in original).

129. *Id.*

130. *Id.* at 731.

131. *Id.* at 732–33.

132. *Id.* at 733.

Defense counsel also sought communications made by the prosecution's key witness to impeach her anticipated testimony at trial on the ground that she was "motivated by jealous rage" to improperly identify Sullivan.[133]

In remanding the case back to the trial court for further determinations, the California Supreme Court emphasized that "in the lower court proceedings the parties did not focus on the public/private configuration distinction."[134] The court instructed the lower court to determine whether any of the communications sought by the defendants were publicly configured.[135] The court suggested that this determination was a necessary prerequisite because, depending on the extent of the publicly configured communications, the defendants might not have had a continuing need for private communications after the publicly configured content was produced.[136] As a result, the court never reached the defendants' constitutional claims.[137]

Similarly, in *Touchstone*, the same court refused to reach the defendant's constitutional claims where there were "questions concerning whether the underlying subpoena [was] supported by good cause."[138] There, the defendant shot his sister's boyfriend and was charged with attempted murder, with additional allegations of personal use of a firearm and inflicting great bodily injury.[139] His counsel sought to subpoena all of the victim's Facebook communications, including restricted posts and private messages, to bolster the defendant's claim of self-defense by revealing the victim's "violent general musings."[140]

The court found the subpoena to be deficient at the outset.[141] In so finding, the court suggested that the posture in this case provided an even weaker vehicle for reaching the attendant constitutional questions than did the *Hunter* case. For example, the court contrasted the insufficient basis for the subpoena in this case with the comparatively "specific basis" for seeking the communications in *Hunter*.[142] The

133. *Id.*
134. *Id.* at 745.
135. *Id.*
136. *Id.*
137. *Id.*
138. Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383, 402 (Cal. 2020).
139. *Id.* at 388.
140. *Id.* at 389–90.
141. *Id.* at 399–401.
142. *Id.* at 398 n.11.

court emphasized that in that case, "there was significant evidence that the underlying shooting and resulting homicide may have related to, and stemmed from, social media posts—and hence the nexus, and justification for intruding into a victim's or witness's social media posts (public and restricted, and/or private messages), was substantial."[143] In contrast, in *Touchstone*, the court found no such specific basis for seeking the communications "beyond identifying general character impeachment evidence."[144] Due to these deficiencies, the court also failed to reach the constitutional claims in this case.

ii. Criminal Defendants Do Not Have a Constitutional Right to SCA-Protected Communications in Pretrial Discovery

When the California Supreme Court takes up a case in which a criminal defendant specifically seeks private, third-party communications pursuant to an otherwise valid subpoena, the court should find that the defendant does not have an overriding constitutional right to that information. "Whether rooted directly in the Due Process Clause of the Fourteenth Amendment, or in the Compulsory Process or Confrontation clauses of the Sixth Amendment, the Constitution guarantees criminal defendants 'a meaningful opportunity to present a complete defense.'"[145] However, both the United States Supreme Court and the California Supreme Court have long recognized that a criminal defendant has no general constitutional right to discovery in a criminal prosecution.[146]

Nevertheless, California courts have found that, generally, a criminal defendant may be entitled to discovery of *non-privileged* information where "it appears reasonable that such knowledge will assist him in preparing his defense."[147] In *People v. Hammon*,[148] the California Supreme Court declined to recognize a constitutional right to pretrial discovery where the defendant was seeking disclosure of statutorily-privileged psychotherapy information.[149] The court noted that

143. *Id.* at 398.

144. *Id.* at 398 n.11.

145. Crane v. Kentucky, 476 U.S. 683, 690 (1986) (citations omitted) (quoting California v. Trombetta, 467 U.S. 479, 485 (1984)).

146. Weatherford v. Bursey, 429 U.S. 545, 559 (1977); People v. Valdez, 281 P.3d 924, 947 (Cal. 2012) (quoting *Weatherford*, 429 U.S. at 559); People v. Maciel, 304 P.3d 983, 1006 (Cal. 2013) (same); People v. Mena, 277 P.3d 160, 170 (Cal. 2012) (same).

147. *Touchstone*, 471 P.3d at 398.

148. 938 P.2d 986 (Cal. 1997).

149. *Id.* at 992–93.

a defendant's general statutory right to issue subpoenas to compel information from private persons "provides no basis for overriding a statutory and constitutional privilege."[150]

This holding extends beyond the psychotherapist-patient privilege. The California Supreme Court has routinely relied on *Hammon* to support the proposition that a criminal defendant is not entitled to pretrial discovery of all types of privileged and confidential information in criminal cases.[151] Thus, in *Touchstone*, the California Supreme Court explained that in arguing that criminal defendants have a constitutional right that overrides the SCA's statutory prohibition on disclosure, the defendant was essentially asking the court to limit or overrule the holding in *Hammon*.[152] The court also recognized that these constitutional claims and arguments were the same as those presented, but not reached, in *Hunter*.[153]

Accordingly, *Hammon*—precedent from California's highest court—lends support for the proposition that criminal defendants do not have an overriding constitutional right to private communications shielded by the SCA. In 2017, before *Touchstone* was appealed to the California Supreme Court, the California Court of Appeal addressed the defendant's constitutional claims and reached the very same conclusion.[154] Initially, the Court of Appeal examined the defendant's constitutional claims concerning his Sixth Amendment right to confrontation.[155] The court noted that based on the principles articulated in *Hammon*, a criminal defendant is generally not entitled to pretrial discovery of any kind,[156] let alone confidential or privileged information. Applying these principles in *Touchstone*, the Court of Appeal found that the defendant was not entitled to pretrial disclosure of SCA-protected communications because the Confrontation Clause does not "mandate[] disclosure of *otherwise privileged information* for

150. *Id.* at 993.

151. Valdez, 281 P.3d at 944–47 (no constitutional violation in withholding witnesses' identities before trial); Alvarado v. Superior Ct. 5 P.3d 203, 211–12 (Cal. 2000) (same); *Maciel*, 304 P.3d at 1006–07 (same); People v. Martinez, 213 P.3d 77, 116 n.13 (Cal. 2009) (Sixth Amendment does not require granting a pretrial discovery motion for juvenile records); People v. Prince, 156 P.3d 1015, 1055 n.10 (Cal. 2007) (defendant's Sixth Amendment claim to pretrial discovery of an FBI database on "weak footing"); People v. Anderson, 22 P.3d 347, 370 n.11 (Cal. 2001) ("[T]he confrontation clause gives no right to pretrial discovery that would override a statutory or constitutional privilege.").

152. *Touchstone*, 471 P.3d at 387.

153. *Id.* at 387–88.

154. Facebook, Inc. v. Superior Ct. (*Touchstone*), 223 Cal. Rptr. 3d 660, 668 (Ct. App. 2017).

155. *Id.* at 667–68.

156. *See id.* (collecting cases).

purposes of [a defendant's] pretrial investigation of the prosecution's case."[157] Thus, the court treated the SCA's prohibitions on disclosure like a statutory privilege.[158] By extension, under *Hammon*, Touchstone had no overriding constitutional right to SCA-protected information.

Next, the court evaluated whether due process requires disclosure of information otherwise protected by the SCA. The court's treatment of the SCA's prohibitions as a statutory privilege also informed its due process analysis. The court explained that defendants do not have an unlimited, due process right to present any and all evidence that may be relevant to their case. State and federal legislators "have broad latitude under the Constitution to establish rules excluding [relevant] evidence from criminal trials."[159] This includes the creation of statutory privileges. Thus, the court squarely rejected Touchstone's assertion that the SCA "must allow a mechanism through which criminal defendants can gain access to the same records routinely obtained by the prosecution and the government."[160]

Acknowledging the procedural variances created by the SCA, the court emphasized that a criminal prosecution "is in no sense a symmetrical proceeding."[161] Instead, the system involves "substantial affirmative obligations and . . . numerous restrictions" on the prosecution that favor the defendant, but also "important aspects of the Government's law enforcement power that are not available to the defendant."[162] In other words, in various aspects of a criminal prosecution, the government and the defense must contend with unilateral restrictions, and thus, have different toolboxes at their disposal. This is not unique to the SCA. Accordingly, the court held that Touchstone's constitutional challenges to the SCA "lack[ed] merit."[163] In addition, the court found that the Supremacy Clause actually *requires* that

157. *Id.* (emphasis added).

158. This treatment is in line with United States Supreme Court precedent. *See* Baldrige v. Shapiro, 455 U.S. 345, 360–61 (1982) (finding that a statutory discovery privilege exists where the statute's text evidences a "strong policy of nondisclosure"); *see also* Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721, 2746–47, 2753 (2020) (arguing that (1) a statutory privilege may be inferred where the practical effect of the statute is that relevant evidence is preemptively excluded, regardless of substance; and (2) courts have read the SCA as impliedly creating an evidentiary privilege).

159. *Touchstone*, 223 Cal. Rptr. 3d at 668.

160. *Id.* at 671.

161. *Id.*

162. *Id.*

163. *Id.* at 674.

California's discovery laws be enforced in a way that does not compel a provider to make disclosures in violation of the SCA.[164]

### iii. Defendants Can Often Obtain a Third Party's Social Media Information Through Alternative Means

Constitutional challenges to the SCA also fail because defendants have a range of options outside the SCA to obtain third-party, social-media information from providers. A criminal defendant's alternatives can be separated into three general buckets: (1) information that the criminal defendant can obtain directly from providers; (2) evidence that the prosecution must turn over to the defense; and (3) information that the criminal defendant can obtain by going directly to the source.

First, the SCA does not bar a criminal defendant from obtaining non-content records and publicly configured communications directly from providers. In fact, the SCA expressly allows ISPs to voluntarily disclose non-content records to non-governmental entities.[165] Criminal defendants (as private parties) can seek disclosures of non-content information, such as the IP addresses of government informants and the friends lists of alleged co-conspirators, without the burden of the compulsory process that the government must use to gain access to the same information.[166] As emphasized by the California Supreme Court in *Hunter*, the SCA also does not prevent a criminal defendant from seeking out publicly configured communications.[167] Moreover, where a social media user is deemed to have consented to disclosure by virtue of her publicly configured communications, California precedent dictates that providers are *required* to disclose this information in response to a valid subpoena.[168] This is also true for non-content records.[169]

Second, under *Brady v. Maryland*,[170] the prosecution must turn over any social media information in its possession that could

164. *Id. See generally*, U.S. CONST. art. VI (establishing that the federal constitution and federal law generally take precedence over state laws and state constitutions).

165. 18 U.S.C. § 2702(c)(6) (2018).

166. Zwillinger & Genetski, *supra* note 55, at 590.

167. Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 744 (Cal. 2018) ("[S]ection 2702(b)(3)'s . . . lawful consent exception allows providers to disclose communications configured by the user to be public.").

168. *See id.* at 751 ("Insofar as the [SCA] permits a given disclosure, it permits a court to compel that disclosure under state law." (quoting Negro v. Superior Ct., 179 Cal. Rptr. 3d 215, 234 (Ct. App. 2014))).

169. *Id.* at 751–52.

170. 373 U.S. 83 (1963).

potentially help the defense. The *Brady* doctrine acts as a limit on the basic rule that criminal defendants have no general constitutional right to discovery in a criminal case.[171] Under *Brady* and its progeny, a criminal defendant *does* have an affirmative, constitutional right to the disclosure of potentially exculpatory evidence.[172] Taking non-content records and publicly configured communications out of the mix, private communications are the only type of information that remain out of reach for a criminal defendant. But, under *Brady*, a criminal defendant even retains some access to this subset of information. As it pertains to the SCA, *Brady* is a catchall that applies equally to non-content records, publicly configured communications, and private communications. Thus, once the government has compelled disclosure of a victim's or witness's social media information pursuant to the SCA, it must turn over *any* information—including private communications—that might be helpful to the defense.

Finally, a criminal defendant can avoid the issues associated with the SCA's prohibitions by subpoenaing the originator or recipient of the desired information, rather than going around them to the non-party providers.[173] This avenue is admittedly impractical in certain situations, for example, where the intended subject of the subpoena is deceased; will refuse to comply; will assert privilege or his Fifth Amendment right against self-incrimination; cannot be located; or where notification could cause witness or evidence tampering.[174] But courts have a variety of tools at their disposal to enforce compliance, such as holding the subject in contempt; imposing fees; or ordering an account holder to provide "lawful consent" for SCA purposes.[175] In

171. Weatherford v. Bursey, 429 U.S. 545, 559 (1977); People v. Valdez, 281 P.3d 924, 947 (Cal. 2012) (quoting *Weatherford*, 429 U.S. at 559); People v. Maciel, 304 P.3d 983, 1006 (Cal. 2013) (same); People v. Mena, 277 P.3d 160, 170 (Cal. 2012) (same).

172. *Brady*, 373 U.S. at 87.

173. *See* CAL. PENAL CODE § 1326(a)(1)–(4) (West 2020) (criminal defendants can issue subpoenas to non-parties, and trial courts can enforce compliance); O'Grady v. Superior Ct., 44 Cal. Rptr. 3d 72, 89 (Ct. App. 2006) (even when the SCA precludes disclosure by a provider, it "does not render the data wholly unavailable; it only means that the discovery must be directed to the owner of the data," not the provider).

174. *See, e.g.*, Zwillinger & Genetski, *supra* note 55, at 592–93; Wexler, *supra* note 158, at 2741.

175. *See, e.g.*, CAL. PENAL CODE § 1331 (West 2020) (a court may enforce contempt of court and fees); CAL. PENAL CODE § 1054.5(b) (West 2018) (court may enforce immediate disclosure, contempt proceedings, delaying or prohibiting witness testimony or presentation of evidence, continuance of the matter, or any other lawful order); Negro v. Superior Ct., 179 Cal. Rptr. 3d 215, 230 (Ct. App. 2014) (holding that consent expressly given by the account holder pursuant to court order constituted lawful consent under the SCA); Juror No. One v. Superior Ct., 142 Cal. Rptr. 3d 151, 159 (Ct. App. 2012) ("If the court can compel Juror Number One to produce the information,

sum, to the extent that non-content records, publicly configured communications, and *Brady* material—in conjunction—are insufficient for a defendant seeking to build his defense, going directly to the source can also be an option.

### *C. Policy Concerns: A Criminal-Defendant Exception Is Dangerous, Deters Victim Participation, and Erodes Internet Privacy*

The policy implications of permitting criminal defendants to circumvent SCA protections by obtaining private, third-party social media communications also militate against the creation of a judge-made exception. Such an exception would place the safety of victims and witnesses in jeopardy and run afoul of the spirit of the legislation, which was crafted for the purpose of providing Fourth Amendment-like privacy protections for internet users.

Becoming a victim of a crime, especially violent crime, is undoubtedly one of the most harrowing events one can experience. The trauma of the experience is often magnified when the victim is forced to relive the crime during the accompanying prosecution.[176] Creating a criminal-defendant exception to the SCA would add insult to injury by placing the victim in a position where the keeper of her most intimate social media communications can bare that information to the perpetrator of the crime. In other words, a criminal-defendant exception, under which a defendant can go around a victim's back to obtain her private internet communications, revictimizes the victim.[177] Such a structure takes control away from the victim, who is best situated to challenge a subpoena for her private information and to assert any

it can likewise compel Juror Number One to consent to the disclosure by Facebook."); Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 657 (Sup. Ct. 2010) (ordering user to provide consent for opposing counsel to access his Facebook posts); *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 614 n.5 (E.D. Va. 2008) (holding that a court "could order the [users] to consent to AOL's disclosing the contents of their e-mails under the pain of sanctions"); Glazer v. Fireman's Fund Ins. Co., No. 11 CIV. 4374, 2012 WL 1197167, at *3 (S.D.N.Y. Apr. 5, 2012) (holding that court "need not determine" whether a user's communications were protected under SCA because the court could "simply *direct* that [the user] consent to disclosure").

176. *See generally* Meg Garvin and Sarah LeClair, *Polyvictims: Victims' Rights Enforcement as a Tool to Mitigate "Secondary Victimization" in the Criminal Justice System*, NAT'L CRIME VICTIM L. INST. 1 (Mar. 2013), https://law.lclark.edu/live/files/13798-polyvictims-victims-rights-enforcement-as-a-tool [https://perma.cc/9MY2-DSAV] (describing how a crime victim's interaction with the criminal justice system can cause revictimization, or "secondary victimization").

177. *See* Meg Garvin et al., *Protecting Victims' Privacy: Moving to Quash Pretrial Subpoenas Duces Tecum for Non-Privileged Information in Criminal Cases*, NAT'L CRIME VICTIM L. INST. 1 (Sept. 2014), https://law.lclark.edu/live/files/18060-quashing-pretrial-subpeonasbulletinpdf [https://perma.cc/26CM-E8W5].

applicable privileges.[178] Moreover, victims have federal and state constitutional and statutory rights to privacy and to be treated with fairness, dignity, and respect.[179] In California, this specifically includes the right to "prevent the disclosure of confidential information or records to the defendant . . . which could be used to locate or harass the victim or the victim's family . . . *or which are otherwise privileged or confidential by law*."[180] To the extent that California courts have already treated the SCA's prohibition on disclosure like a statutory privilege, this is not only in line with the SCA's underlying policy, but also the policy concerns that led to an increase in protections for victims in California.[181]

In many situations, the disclosure of a victim's or witness's private social media communications to the defendant can be dangerous. For example, in a domestic violence case, disclosing a victim's private communications to a defendant, who may be out of custody on bond,[182] can aggravate an already precarious situation for the victim.[183] Likewise, in a gang-related violent crime, a criminal defendant who is given access to a key witness's sensitive information can enlist his friends to engage in witness intimidation.

178. *See* Facebook, Inc. v. Wint, 199 A.3d 625, 631 (D.C. 2019) ("[C]hanneling such discovery to senders or recipients, rather than providers, increases the chances that affected individuals can assert claims of privilege or other rights of privacy before covered communications are disclosed to criminal defendants in response to subpoenas.").

179. *See* Garvin et al., *supra* note 177, at n.5 (collecting cases); 18 U.S.C. § 3771(a)(1) (2018) (crime victims have a right to reasonable protection from the accused); CAL. CONST. art. I, § 28(b).

180. CAL. CONST. art. I, § 28(b)(4) (emphasis added).

181. *See generally Marsy's Law*, CAL. DEP'T OF CORR. & REHAB., https://www.cdcr.ca.gov/victim-services/marsys-law/ [https://perma.cc/2BTN-8Y54] ("On November 4, 2008, the People of the State of California approved Proposition 9, the Victims' Bill of Rights Act of 2008: Marsy's Law. This measure amended the California Constitution to provide additional rights to victims."); MARSY'S CARD AND RESOURCES, CAL. ATT'Y GEN.'S OFF. (Oct. 2017), https://oag.ca.gov/sites/all/files/agweb/pdfs/victimservices/marsy_pocket_en_res.pdf [https://perma.cc/UZ69-KA2E] (card containing instructions and resources provided to all California crime victims).

182. *See, e.g.*, Jason Pohl, *'Unconscionable.' How a Surge in Domestic Violence Is Saving the Bail Bond Industry*, Sacramento Bee (Oct. 12, 2020, 7:51 AM), https://www.sacbee.com/news/politics-government/article246124355.html [https://perma.cc/7YWD-2WQS] (In Sacramento, between April and October 2020, "[r]oughly 42% of all of the people who bonded out of jail . . . were released while facing at least one charge related to domestic violence.").

183. *See, e.g.*, NAT'L INST. OF JUST., U.S. DEP'T OF JUST., PRACTICAL IMPLICATIONS OF CURRENT DOMESTIC VIOLENCE RESEARCH: FOR LAW ENFORCEMENT, PROSECUTORS AND JUDGES 21 (June 2009), https://www.ojp.gov/pdffiles1/nij/225722.pdf [https://perma.cc/5B7C-RZTH] ("In states where no-contact orders are automatically imposed after an arrest for domestic violence, rearrests for order violations begin to occur immediately upon the defendant's release from the police station or court . . . . A multistate study of abusers referred to batterer programs found that almost half of the men (44 percent) who reassaulted their partners did so within three months of batterer program intake, and two-thirds within six months.").

Not only would a criminal-defendant exception to the SCA be unjustifiably invasive and dangerous, it would also deter victim and witness reporting and participation. The criminal justice system depends on the assistance of victims and witnesses. In addition to testifying for the government, victims and witnesses also participate informally by providing prosecutors with vital information.[184] Victims and witnesses are less likely to report crimes and to cooperate with the government's investigation and prosecution if they know that doing so would expose them to an intrusive sweep of their most intimate communications by the defense.[185]

Moreover, in enacting the SCA, Congress sought to "ensure the continued vitality of the fourth amendment" and to prevent the "gradual erosion" of the privacy rights of internet users.[186] If criminal defendants are to be permitted to compel private, third-party communications from social media providers, the gradual erosion feared by Congress would instead resemble a complete breakdown of the foundation on which our internet privacy protections rest. Social media has become a ubiquitous forum for our most intimate communications. In 2021, 72 percent of Americans reported using at least one social media site.[187] For many Americans, social media is a repository of self. Similar to a diary or a love letter, the private-messaging platforms housed within these sites contain the most intimate expressions of that self. Thus, the prospect of permitting criminal defendants to wade through those communications, which the sender never expected anyone but the recipient to view, is the highest form of privacy invasion.

In effect, a criminal-defendant exception to the SCA would provide unfettered access to the contents of a victim's or witness's private communications. Where communications are not only private, but also do not include the defendant as a sender or recipient, the defense has no way of knowing with any certainty what sort of information it will find once it begins looking. Presumably, the defense would be sifting through a large body—if not the entirety—of a victim's or witness's private exchanges, looking for a proverbial needle in a haystack that

184. *See* Robert C. Davis et al., *Expanding the Victim's Role in the Criminal Court Dispositional Process: The Results of an Experiment*, 75 J. CRIM. L. & CRIMINOLOGY 491, 492 (1984).

185. *See* Garvin et al., *supra* note 177, at 1.

186. S. REP. NO. 99-541, at 5 (1986).

187. *Social Media Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021) https://www.pewresearch.org/internet/fact-sheet/social-media/ [https://perma.cc/8MYJ-L45S].

might not even exist.[188] In the process, the victim's or witness's most intimate communications with a third-party, who is even further removed from the underlying criminal prosecution, will be completely exposed.

Finally, the creation of a criminal-defendant exception touches every social media user, and not just the narrower subset of those who might end up as victims of, or witnesses to, a crime. If a criminal defendant is entitled to access the private communications between a victim or witness and any other third party, then the SCA's privacy protections, on which all social media users have come to rely, are merely illusory. None of our social media communications are truly private where, at any point, they may be dissected because the person on the other end happened to be the victim of, or witness to, a crime.

## V. CONCLUSION

A criminal defendant does not have a right—under the SCA, the Fifth and Sixth Amendments, or otherwise—to private, third-party social media communications in pretrial discovery. Arguments to create a carve-out for criminal defendants are incompatible with the plain text of the statute, unsupported by the constitutional interpretations of the courts, and contrary to the purposes of the SCA. When the California Supreme Court litigates the constitutionality of the SCA in relation to criminal defendants' pretrial requests for disclosures of private social media communications, it should hold that the creation of a judge-made, criminal-defendant exception is not constitutionally mandated, is contrary to both California precedent and the SCA, and cannot stand.

188. Courts are authorized to refuse to enforce subpoenas for information that constitute "fishing expeditions" to see what may turn up. *See* Garvin et al., *supra* note 177, at 3 (citing United States v. Nixon, 418 U.S. 683, 699 (1974)).