# THE LIMITATIONS OF APPLYING THE STORED COMMUNICATIONS ACT TO SOCIAL MEDIA

VICTORIA M. ALLEN*

ABSTRACT

*The advent of social media has increasingly affected how people live and communicate. Millions of Americans use social media every day, and the numbers continue to grow. The motivation to post on social media is multifactorial and includes a desire to stay connected, find others with shared interests, change opinions, and encourage action, but posting also serves to boost one's self-esteem and self-worth. However, posting on social media creates a serious risk of self-disclosure, with people revealing more intimate details online than they would in more traditional settings without really appreciating the privacy issues and potential negative consequences related to such disclosures.*

*As social media use continues to grow, its use as a tool in police investigations has also increased. Both the content and metadata associated with social media posts now routinely aid law enforcement authorities in finding patterns and, importantly, in establishing timelines in criminal investigations. Thus, there is an urgent need to revise the existing laws governing stored communications—to better adapt them to these new, evolving technologies and improve the legal framework governing online privacy rights. This Note argues that various aspects of the Stored Communications Act ("SCA") are outdated and that thirty-six years after it was enacted, it is time for an update that reflects the changing landscape of evolving technological advances.*

* Executive Senior Editor, *Southern California Law Review*, Volume 96; J.D. Candidate 2023, University of Southern California Gould School of Law; M.S. Clinical Research Methods 2020, Fordham University; B.A. Psychology 2015, New York University. My thanks to my parents, Marlene and Lee Allen, and Jennifer Guillen for their input and support throughout the note-writing process. I would also like to thank my Note advisor, Professor Eileen Decker, for her guidance, and the members of the *Southern California Law Review* for their hard work and thoughtful suggestions.

*The Note explores how the internet and social media use have evolved over the years and explains why the SCA no longer sufficiently protects consumers from government acquisition of their information. Particular emphasis is placed on the novelty of social media "Stories," a technology unlike any that Congress could have imagined when it enacted the SCA in 1986. The Note examines the history of the SCA—with a focus on the Fourth Amendment, the Electronic Communications Privacy Act, and Supreme Court cases addressing the applicability of the Fourth Amendment to various forms of communication technology—before analyzing the SCA in detail, and looks at how law enforcement agencies can obtain these communications for use in criminal investigations. The Note concludes by arguing that the SCA needs to be revised to more adequately apply to today's social media technologies since their content, and non-content, does not easily fit into the currently delineated categories. Revising the SCA would afford greater protection to consumer communication rights: not only would the SCA better apply to modern technology, but it would also be more readily applicable to future emerging media technologies.*

TABLE OF CONTENTS

## INTRODUCTION

The rise of social media has significantly impacted the way people live and communicate, and the trend toward extensive social media use will likely only continue to grow. According to a Pew Research Center study, seven in ten Americans use social media.[1] On average, people spend an estimated two and a half hours on social media platforms over the course of their day,[2] and "[a] majority of Facebook, Snapchat and Instagram users say they visit these

1. Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021 [https://perma.cc/DG7C-4FY3].

2. *Global Social Media Statistics*, DATAREPORTAL, https://datareportal.com/social-media-users [https://perma.cc/Y6JS-XZQF]. While this number might not seem large when compared to the twenty-four hours in the day, it is reported that, on average, Americans spend around five and a half hours a day on their phones, while globally, people average just over three hours of phone time per day. Damjan Jugović Spajić, *How Much Time Does the Average Person Spend on Their Phone?*, KOMMANDO TECH (May 10, 2022), https://kommandotech.com/statistics/how-much-time-does-the-average-person-spend-on-their-phone [https://perma.cc/K5HZ-W9TF]. This means that of all the time people spend on their phones each day, about one half is spent exclusively on social media.

platforms on a daily basis."[3] More specifically, 69% of Americans use Facebook, 40% of Americans use Instagram, and 25% of Americans use Snapchat.[4] These percentages represent a significant number of people—approximately 230 million, 133 million, and 83 million, respectively.[5] Further, social media users make extensive use of the "Stories"[6] feature, with one billion Facebook Stories being posted daily and five hundred million daily active users of Instagram Stories worldwide.[7] The motivation to post on social media is multifactorial and includes a desire to stay connected, find others with shared interests, change opinions, and encourage action, but posting also serves to boost one's self-esteem and self-worth.[8] These desires create a serious risk of self-disclosure on social media, with people revealing more intimate details online than they would in more traditional settings without really appreciating the privacy issues and potential negative consequences related to such disclosures.

Just as social media has become popular with the American public, it is also becoming increasingly utilized as a tool in police investigations. A 2012 survey showed that four out of five law enforcement agents used social media to gather intelligence during investigations.[9] Not only do authorities look online for public information, but they also request access to private data directly from social media providers—which can help them build their criminal cases. For example, after finding photos and comments "glamorizing alcohol abuse" on a woman's MySpace page, prosecutors were able to use them as evidence and advocate for a longer sentence for her vehicular manslaughter conviction.[10] Since people are less inhibited when it comes to social media disclosures, they often share details of their lives and more controversial opinions than they may in other forums. After these once private thoughts are stored electronically, they become more easily

3. Auxier & Anderson, *supra* note 1.

4. *Id.*

5. These numbers were calculated based on the Census Bureau's most recent estimate of the American population (332,403, 650). Derrick Moore, *U.S. Population Estimated at 332,403,650 on Jan. 1, 2022*, U.S. CENSUS BUREAU (Dec. 30, 2021), https://www.census.gov/library/stories/2021/12/happy-new-year-2022.html [https://perma.cc/3Z3P-3HVB].

6. *See infra* Section I.B.

7. Jimit Bagadiya, *430+ Social Media Statistics You Must Know in 2022*, SOCIALPILOT, https://www.socialpilot.co/blog/social-media-statistics [https://perma.cc/D6DJ-SPU9].

8. Rosalyn Ransaw, *The Psychology Behind Why We Share on Social Media*, SHUTTERSTOCK (Apr. 30, 2021), https://www.shutterstock.com/blog/the-psychology-behind-why-we-share-on-social-media [https://perma.cc/9B4D-72D7].

9. Heather Kelly, *Police Embrace Social Media as Crime-Fighting Tool*, CNN BUSINESS (Aug. 30, 2012, 5:23 PM), https://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html [https://perma.cc/2EPT-56GK].

10. Ian Urbina, *Social Media, a Trove of Clues and Confessions*, N.Y. TIMES (Feb. 15, 2014), https://www.nytimes.com/2014/02/16/sunday-review/social-media-a-trove-of-clues-and-confessions.html [https://perma.cc/9BRM-HGAD].

accessible to investigators. Not only can the content of social media posts aid criminal investigations, but the related metadata[11] alone "can help law enforcement authorities to find patterns, establish timelines and point to gaps in the data."[12] Therefore, social media metadata can be just as easily used to gather information on a suspect as the actual content of a post. Because the trend toward extensive social media use will likely endure, there is an urgent need to revise the laws governing stored communications—to better adapt them to these evolving technologies and improve the legal framework governing online privacy rights.

This Note argues that various aspects of the Stored Communications Act ("SCA") are outdated and that thirty-six years after it was enacted, it is time for an update that reflects the changing landscape of evolving technological advances. Part I of this Note explores how the internet and social media have evolved throughout the years and explains why the SCA no longer affords sufficient protections against government acquisition of consumer information. It discusses the evolution and expansion of social media platforms. Particular emphasis is placed on the novelty of social media Stories, which are unlike any technology that Congress could have imagined when they enacted the SCA in 1986.

Next, Part II examines the history behind the SCA to explain why the law was initially passed by Congress, with a focus on the Fourth Amendment, the Electronic Communications Privacy Act ("ECPA"), and Supreme Court cases addressing the applicability of the Fourth Amendment to various forms of technology. Part III analyzes the SCA in detail, focusing on the distinctions made between the different types of internet service providers ("ISPs") and the different aspects of communications (content versus non-content data). It looks at how the content and non-content information—for example, metadata including a user's identity, location, and other data not part of the main substance of the communication—can be obtained by law enforcement in the course of a criminal investigation.

Part IV argues that the SCA cannot be easily applied to social media

11. There are different kinds of metadata, but in the context of criminal investigations and social media, descriptive metadata—which includes the time and date the content was created and posted, the creator of the data, and the location on the device where the data was created—can be implicated. *Metadata Forensics, When Files Can Speak and Reveal the Truth*, IRONHACK (June 24, 2021), https://www.ironhack.com/en/cybersecurity/metadata-forensics-when-files-can-speak-and-reveal-the-truth [https://perma.cc/8XWX-HEKD].

12. Adelle Geronimo, *Beyond Data: The Value of Metadata in Criminal Investigations*, ITP.NET (Sept. 1, 2021), https://www.itp.net/security/99783-beyond-data-the-value-of-metadata-in-criminal-investigations [https://perma.cc/SVB6-QE42]. "[C]hanging technology has rendered metadata analysis more important." Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 398 (2014).

today because it does not fit within the categories delineated in the SCA. Most importantly, it highlights how (1) social media content does not easily fit into either of the SCA's currently defined categories because Congress could not have anticipated the advances in the technologies that exist today; and (2) "non-content" is not fully defined in the statute, and therefore lends itself to being more easily obtained in some situations as opposed to others. Finally, Part V suggests ways in which the SCA can be revised to more adequately apply to social media today and ultimately protect the right to privacy guaranteed by the U.S. Constitution.

## I. INTERNET PRIVACY AND EVOLVING TECHNOLOGY

Americans are entitled to their right to privacy, which on third-party ISPs such as Facebook and MySpace is protected by the SCA.[13] One problem with the SCA, however, is that it is dated. Although the internet was invented in the 1960s, it was not widely used until 1983, when computers on different networks were finally able to easily communicate with one another.[14] When the SCA was enacted in 1986—just three years later—Congress had only a limited experience with internet use and the potential privacy problems it could create, and had certainly not envisioned the extensive modern use of social media. This partially accounts for some of the weaknesses in this legislation and why the SCA is often difficult to apply to social media today.

### A. EVOLUTION OF SOCIAL MEDIA PLATFORMS

Social media is defined as "forms of electronic communication . . . through which users create online communities to share information, ideas, personal messages, and other content."[15] This definition implies that social media could not exist without the internet, and that it depends on user-generated content.[16] While it can be said that social media began in 1971, when the first email was sent,[17] for many people social media really began in the late 1990s or early 2000s—years after the SCA was enacted—with the advent of messaging services such as AOL and MSN

13. Stored Communications Act, 18 U.S.C. §§ 2701–2713.

14. *A Brief History of the Internet*, BD. OF REGENTS OF THE UNIV. SYS. OF GA., https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml [https://perma.cc/P72B-H2DS].

15. *Social Media*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/social%20media [https://perma.cc/3PUC-PTPT].

16. *See* Matthew Jones, *The Complete History of Social Media: A Timeline of the Invention of Online Networking*, HIST. COOP. (June 16, 2015), https://historycooperative.org/the-history-of-social-media [https://perma.cc/WUZ9-JVWE].

17. Rachel Swatman, *1971: First Ever Email*, GUINNESS WORLD RECS. (Aug. 19, 2015), https://www.guinnessworldrecords.com/news/60at60/2015/8/1971-first-ever-email-392973 [https://perma.cc/9CNE-U852].

Messenger.[18] MySpace, arguably the "most popular and influential" of the early social media platforms, was later launched in August 2003,[19] and it allowed individuals to interact by commenting on each other's profiles and sending private messages. It was the largest social media platform until Facebook, created in 2004, overtook it in 2008.[20] Facebook has now grown to be the largest social media platform in the world with almost three billion monthly active users.[21]

The number and types of social media platforms have grown extensively. Today, other prominent social media platforms include Instagram and Snapchat. Instagram was launched in 2010 and is a platform focused on sharing photos and videos.[22] Snapchat was created in 2011 and gained its popularity from users' ability to send each other pictures or videos ("Snaps") that disappear shortly after being opened.[23] These platforms allow users to share content with their friends, some of which they believe to be "private," visible only to those friends they allow to see it. However, the widespread use of these platforms has created new issues with how the government can legally access and use these communications.

### B. EMERGENCE OF STORIES ON SOCIAL MEDIA PLATFORMS

The continued evolution and development of new information sharing functions on social media platforms have created multiple issues concerning user privacy rights. For example, in 2013, Snapchat began to allow people to share "Stories" that are displayed for twenty-four hours before becoming inaccessible.[24] Stories are a collection of individual Snaps that are played in

18. *See* Caitlin Dewey, *A Complete History of the Rise and Fall—and Reincarnation!—of the Beloved '90s Chatroom*, WASH. POST (Oct. 30, 2014, 2:01 PM), https://www.washingtonpost.com/news/the-intersect/wp/2014/10/30/a-complete-history-of-the-rise-and-fall-and-reincarnation-of-the-beloved-90s-chatroom [https://perma.cc/PB3Y-4T3B] ("Services like MSN and AOL . . . made the chat function available to millions of Americans . . . .").

19. Jones, *supra* note 16; Nicholas Jackson & Alexis C. Madrigal, *The Rise and Fall of MySpace*, ATLANTIC (Jan. 12, 2011), https://www.theatlantic.com/technology/archive/2011/01/the-rise-and-fall-of-myspace/69444 [https://perma.cc/ZYJ4-9NEJ]. Although MySpace was more popular, Six Degrees is "credited as being the 'first online social media' site" because it "allowed people to sign up with their email address, make individual profiles, and add friends to their personal network." Jones, *supra* note 16. Six Degrees only lasted for four years, and it peaked at less than four million users, *id.*, far less than the twenty-seven million users MySpace had just two years after its launch. Jackson & Madrigal, *supra*.

20. Jones, *supra* note 16.

21. *Facebook Statistics and Trends*, DATAREPORTAL, https://datareportal.com/essential-facebook-stats [https://perma.cc/BP76-FY42] ("Facebook had 2.934 billion monthly active users in July 2022 . . . .").

22. Jones, *supra* note 16.

23. *Id.*

24. Emma Wiltshire, *The Rise of the Story Format [Infographic]*, SOCIAL MEDIA TODAY (Feb. 2, 2018), https://www.socialmediatoday.com/news/the-rise-of-the-story-format-infographic/516143 [https://perma.cc/SWJ6-9MXN].

the order in which they were created and allow users to share their entire day in a narrative manner. Today, Stories are also available on a variety of other social media platforms, including Facebook and Instagram.[25] Part of the reason why Stories are so successful is because they are only available temporarily, so people can post small daily updates or silly images that they only want visible for a short period of time.[26] Therefore, users reasonably believe that their content will remain private and then disappear, becoming permanently inaccessible. Another reason for the success of Stories is that "social media [S]tories tend to be more spontaneous" than an individual's carefully curated feed, making it feel more "casual."[27] As a result, these Stories can be extremely useful to law enforcement, as they can provide a less filtered view of an individual's daily life and a timeline for the posted events. Thus, the challenge becomes balancing users' right to privacy with the government's need for access to information in order to investigate criminal offenses.

As it exists now, the SCA does not provide an adequate statutory framework for protecting communications on the various aforementioned social media platforms and, importantly, does not specifically address new advances in technology such as transient Snapchat and Instagram Stories. Since the SCA does not adequately protect individuals from unlawful searches of their private social media data, there is a need for Congress to reform the statute to accommodate evolving technology.

## II. HISTORY OF THE STORED COMMUNICATIONS ACT

### A. THE FOURTH AMENDMENT

The Fourth Amendment to the Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[28] While the meaning of "search" is not immediately defined by the Amendment, the Supreme Court has held that "[a] 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed"[29] and that "[i]f the inspection by police

25. Snapchat was the first social media platform to utilize Stories, in October 2013, with Instagram following in August 2016 and Facebook in March 2017. *Id.* Other social media applications have also started utilizing Stories. *Id*.

26. *See* Simon Batt, *What Are "Stories" on Social Media?*, MAKE TECH EASIER (Jan. 3, 2019), https://www.maketecheasier.com/stories-on-social-media [https://perma.cc/AD66-7R7A] (noting the traits that make Stories useful).

27. Chloe West, *Social Media Stories: Your Guide to All Social Media Story Platforms*, SPROUT SOC. (June 30, 2021), https://sproutsocial.com/insights/social-media-stories [https://perma.cc/EV8W-C9LD].

28. U.S. CONST. amend. IV.

29. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

does not intrude upon a legitimate expectation of privacy, there is no 'search.' "[30] Thus, when it comes to physical searches, the meaning of the Fourth Amendment is well understood,[31] whereas what constitutes a search in the digital context is more uncertain.

In *Olmstead v. United States*, the Supreme Court held that wiretapping did not violate the Fourth Amendment because the lack of physical trespass and seizure of anything tangible meant there was no search or seizure.[32] Because the Court refused to expand the Fourth Amendment to protect telephone communications,[33] the government could legally intercept citizens' communications as long as they did not physically enter their homes. *Olmstead* was later overruled by *Katz v. United States*,[34] indicating a change in ideology that afforded citizens protection of their privacy even without a physical search. Because *Katz* held that a physical intrusion was not necessary to invoke the Fourth Amendment, online searches—which lack physical intrusions—can still violate the Fourth Amendment.

### B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

In light of these changing viewpoints on the applicability of Fourth Amendment protections, Congress enacted the ECPA[35] in 1986 in an effort to adapt the doctrines of the Fourth Amendment to the various emerging technologies. The SCA, which provides privacy protections to stored electronic and wire communications, is one part of the ECPA. The ECPA was created with the purpose of protecting American citizens from "the unauthorized interception of electronic communications."[36] Congress recognized a need to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[37] Rightly, Congress worried that due to these advances, personal communications could be intercepted by

30. Illinois v. Andreas, 463 U.S. 765, 771 (1983).

31. ORIN S. KERR, COMPUTER CRIME LAW 389 (4th ed. 2018).

32. Olmstead v. United States, 277 U.S. 438, 463–64 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967) (holding that the use of the wiretapped conversations of a suspected bootlegger as incriminating evidence did not violate his Fourth Amendment rights because wiretapping did not constitute a search or seizure under the meaning of the Fourth Amendment since there was no physical trespass).

33. *Id.* at 465.

34. *Katz*, 389 U.S. at 357–59 (holding that putting a recording device in a public phonebooth violated a gambling suspect's Fourth Amendment rights because the Fourth Amendment applies to people, not places).

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

36. S. REP. NO. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

37. *Id.* At the time, advances in technology included "large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing." *Id.* at 2.

individuals who had no right to obtain them, and thus felt it was important to enact the ECPA.[38] However, the scope of the ECPA did not fully anticipate the impact of the growth and extent of social media.

### C. SUPREME COURT CASES ADDRESSING THE FOURTH AMENDMENT AND TECHNOLOGY

More recently, the Supreme Court heard a series of cases that addressed the applicability of the Fourth Amendment to newer technologies. In each of these cases, the Supreme Court Justices grappled with applying the existing legal framework, indicating that it is time for a change. In Justice Sotomayor's concurring opinion in *United States v. Jones*,[39] she emphasized that in the absence of a physical trespass, a Fourth Amendment search occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable."[40] She also argued that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" because "[t]his approach is ill suited to the digital age."[41] Justice Sotomayor's statements highlight the need to reevaluate the applicability of the current legal framework to new technologies.

Two years later, in *Riley v. California*,[42] Justice Roberts acknowledged that because technology enables modern cell phones to contain and potentially reveal a wealth of private information, cell phones require greater privacy protections than would be necessary for a traditional search.[43] Four years after *Riley*, the Court once again addressed warrantless searches in *Carpenter v. United States*, this time through the collection of cell phone records from a third party.[44] Again, Justice Roberts recognized the need for stronger privacy protections, stating that "a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party," such as the cell site records indicating the defendant's location and movements.[45] The government had acquired this information pursuant to a court order issued under the SCA, which was obtained based on evidence

38. *Id.* at 3.

39. United States v. Jones, 565 U.S. 400 (2012) (holding that using a GPS device without a warrant to track an individual's car through public streets was a violation of his Fourth Amendment rights).

40. *Id.* at 414 (Sotomayor, J., concurring) (quoting Kyllo v. United States, 553 U.S. 27, 31–33 (2001)).

41. *Id.* at 417.

42. Riley v. California, 573 U.S. 373, 401 (2014) (holding that a warrantless search of a cell phone conducted incident to arrest violated the Fourth Amendment because "a warrant is generally required before such a search, even when a cell phone is seized incident to arrest").

43. *Id.* at 403.

44. Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018).

45. *Id.* at 2222.

that the information might be relevant to the ongoing investigation.[46] Finding this burden of proof—requiring only that the information might be relevant, which is lower than the probable cause required to obtain a warrant—to be unacceptable, the Court held that to access these cell site records, a warrant was required.[47] The differing standards of proof required to obtain warrants and court orders to access records from these new technologies illustrate that sometimes the SCA troublingly affords lesser protections to individuals' private information.

## III. THE STORED COMMUNICATIONS ACT

The SCA was enacted to regulate electronic and wire communications that are stored on third-party servers[48] and therefore governs the interaction between government investigators and administrators of third-party service providers.[49] It was meant to expand the privacy protections afforded by the Fourth Amendment to digital content, clarifying its applicability. However, the SCA regulates retrospective communications, meaning it only applies when the government seeks to obtain information already in a provider's possession.[50] Additionally, the SCA only applies to two types of ISPs: providers of electronic communication service ("ECS") and providers of remote computing service ("RCS").[51] An ECS is defined as "any service which provides . . . the ability to send or receive wire or electronic communications;"[52] email and cell phone service providers would therefore be examples of ECS providers. An RCS, on the other hand, is defined as any service that provides to the public "computer storage or processing services by means of an electronic communications system."[53] Thus, once an email has been received but not deleted or a voicemail has been left in storage for later review, email and cell phone services are treated as RCS providers. Because ECS and RCS providers are afforded different levels of protection, it is important to be able to appropriately categorize modern ISPs to determine how much protection users' communications will be given.

While transmitting communications and storing communications are different functions, this distinction matters less today, as many modern ISPs provide both services. In 1986, however, Congress was concerned about

46. *Id.* at 2221.
47. *Id.*
48. PRIVACY RIGHTS IN THE DIGITAL AGE 564 (Jane E. Kirtley & Michael Shally-Jensen, eds., 2nd ed. 2019).
49. KERR, *supra* note 31, at 675.
50. *Id.* at 675–76.
51. PRIVACY RIGHTS IN THE DIGITAL AGE, *supra* note 48, at 565.
52. 18 U.S.C. § 2510(15).
53. *Id.* § 2711(2).

businesses such as hospitals and banks using remote computing services to store records and process data.[54] Thus, they felt the need to create the RCS category to address this concern.[55] Generally, the SCA prohibits disclosure of both content and non-content[56] data of customer communications, but the SCA provides exceptions to this rule.[57] These exceptions, which are discussed below, are divided between § 2702, which regulates voluntary disclosure, and § 2703, which regulates required disclosure.

### A. DISCLOSURE OF THE CONTENTS OF SOCIAL MEDIA POSTS

#### 1. Voluntary Disclosure of Customer Communications

Section 2702(b) details the nine circumstances in which a provider may voluntarily disclose the contents of a customer's communications.[58] These exceptions include allowing the contents to be disclosed "to an addressee or intended recipient of such communication" and "with the lawful consent of the originator or an addressee or intended recipient of such communication."[59] For the most part, the communications can be disclosed only with the permission of the sender or intended recipient, which protects the user, or without their permission in the case of an emergency, such as a missing child.[60] Therefore, while individuals are generally protected against voluntary disclosures of their private information by ISPs, it does not mean that the government is unable to obtain this information; it can be compelled through required disclosure under § 2703.

54. S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

55. It is unclear, however, why Congress felt that ECS and RCS communications should be afforded differing levels of protection.

56. Non-content data is information the service provider collects about the subscriber of the service, such as their name and address.

57. Stored Communications Act, 18 U.S.C. §§ 2701–2713.

58. *Id.* § 2702(b)(1)–(9).

59. *Id.* § 2702(b)(1), (3). The other seven instances in which a provider may also divulge the contents of a customer communication are as follows:

> as otherwise authorized in section 2517, 2511(2)(a), or 2703 of [Title 18]; . . . to a person employed or authorized or whose facilities are used to forward such communication to its destination; . . . as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; . . . to a law enforcement agency . . . if the contents . . . were inadvertently obtained by the service provider; and . . . appear to pertain to the commission of a crime; . . . to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency; or . . . to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

*Id.* § 2702(b)(2), (4)–(9).

60. *Id.* § 2702(b)(6).

2. Required Disclosure of Customer Communications

Should the government decide that obtaining an individual's communications is essential for building a criminal case against them, the disclosure of those communications is governed by § 2703.[61] This is where the largest privacy threat to social media users lies, as ISPs are then legally required to turn over the contents of customer communications to law enforcement. How the government goes about getting this information under § 2703, however, depends on a variety of factors, beginning with whether the ISP is categorized as an ECS or an RCS.

If the government requires information from an RCS, there are three ways for it to compel disclosure.[62] First, the government can compel disclosure without notifying the customer if "the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures . . . ) by a court of competent jurisdiction."[63] Alternatively, if the government provides notice to the customer, it can compel disclosure by using either (1) "an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena;" or (2) "a court order . . . [obtained] under subsection [2703](d)."[64] Warrants place a higher burden on the government in order to obtain the requested information, while subpoenas and court orders are more easily obtainable. Thus, allowing the government to choose the second or third method to avoid having to obtain a warrant shifts the burden to the individual, who then must object to the subpoena or court order to protect their private information.

Required disclosure from an ECS, on the other hand, is even more complicated because it also considers information about the age of the communication.[65] If the communication is 180 days old or less, the government may only compel disclosure "pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures . . . ) by a court of competent jurisdiction."[66] If the communication is more than 180 days old, however, the government can compel disclosure with either a warrant or, if prior notice is provided, a subpoena or court order.[67] In effect,

61. *See id.* § 2703.
62. *Id.* § 2703(b).
63. *Id.* § 2703(b)(1)(A).
64. *Id.* § 2703(b)(1)(B).
65. *See id.* § 2703(a); *see also* PRIVACY RIGHTS IN THE DIGITAL AGE, *supra* note 48, at 565.
66. 18 U.S.C. § 2703(a).
67. *Id.*

this makes it easier for investigators to obtain older communications, with no explanation as to why the 180-day mark is significant; thus, in this situation, users are arbitrarily[68] afforded less protections.

### B. DISCLOSURE OF THE NON-CONTENT DATA OF SOCIAL MEDIA POSTS

#### 1. Voluntary Disclosure of Customer Records

Section 2702(a)(3) prohibits ECS and RCS providers from "divulg[ing] a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity."[69] However, § 2702(c) provides an exception to this rule: "A provider . . . may divulge a record or other information pertaining to a subscriber to or customer of such service . . . as otherwise authorized in section 2703."[70] Therefore, while the SCA prevents ECS and RCS providers from voluntarily disclosing non-content information to governmental entities, as with content, the government can still obtain the information by utilizing § 2703's required disclosure provision.

#### 2. Required Disclosure of Customer Records

Section 2703(c)(1) states that a governmental entity can require an ECS or RCS provider to disclose a record or other information when the governmental entity "obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures . . . ) by a court of competent jurisdiction"; "obtains a court order"; "has the consent of the subscriber or customer"; "submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud"; or "seeks information" under § 2703(c)(2).[71] Section 2703(c)(2) allows ECS and RCS providers to disclose the name; address; telephone connection records (or records of session times and durations); length of service and types of service utilized; subscriber number; and "means and source of payment" when the governmental entity "uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or

68. I use the word "arbitrarily" because it is unclear why Congress chose 180 days to delineate between stored communications and contemporaneous communications. There is no information in the congressional record to indicate why 180 days was chosen. *See* S. REP. NO. 99-541 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555. Orin Kerr calls the 180-day rule "strange," and suggests it was chosen by the drafters because they "figured that unretrieved files not accessed after 180 days ha[d] been abandoned." 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, 1234 (2004).

69. 18 U.S.C. § 2702(a)(3).

70. *Id.* § 2702(c).

71. *Id.* § 2703(c)(1).

any means available under [§ 2703(c)](1)]."[72] Again, governmental entities are able to obtain varying amounts of private information about customers from ECS and RCS providers with either a warrant or a court order, sometimes even with only a subpoena. Even more troubling, § 2703(c) does not require the government entity receiving the records or information to provide notice to the customer.[73] Thus, subscribers' privacy may be being infringed without their knowledge, providing them with fewer opportunities to protect themselves.

## IV. SOCIAL MEDIA AND THE STORED COMMUNICATIONS ACT

Prior to 2010, no court had specifically addressed whether social media platforms were within the jurisdiction of the SCA.[74] In order for the SCA to apply to social media platforms, these ISPs must be considered either ECS or RCS providers. The District Court for the Central District of California was the first to examine whether social media platforms were ECS or RCS providers in *Crispin v. Christian Audigier, Inc.*[75] The district court held that because the three social media platforms in question provided either private messaging or email services, they qualified as ECS providers.[76] This demonstrated that the SCA could be applied to social media platforms and can, therefore, be used to control the release of social media communications. While *Crispin* made it clear that Facebook, Instagram, and Snapchat would be governed by the SCA, it remains unclear whether these platforms qualify as an ECS, an RCS, or both, in the context of specific functions. As a result, which regulations should be applied when the government seeks to obtain users' content (or non-content) from social media platforms during a criminal investigation remains uncertain.

### A. OBTAINING CONTENTS OF SOCIAL MEDIA POSTS

#### 1. Obtaining Contents from Private Social Media Accounts

The SCA only applies to communications that are not "readily accessible to the general public."[77] Thus, it is important to understand how a user's varying privacy settings on social media platforms can affect the applicability of the SCA. Facebook, Instagram, and Snapchat each have

72. *Id.* § 2703(c)(2).
73. *Id.* § 2703(c)(3).
74. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 977 (C.D. Cal. 2010).
75. *See id.* at 980.
76. *Id.*
77. 18 U.S.C. § 2511(2)(g) ("It shall not be unlawful under [the SCA] for any person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public . . . .").

varying features that provide users with controls to limit who can see the content they have posted on their individual accounts, in some instances allowing the users to limit who can view individual posts as well, and the ability to block other users from viewing their content.[78] Accordingly, should a user want their social media content to be private, they have the ability to set those limits using the social media platform settings.

In *Crispin*, the court held that "[u]nquestionably, the case law . . . require[s] that [user content] be restricted in some fashion . . . [to] merit protection under the SCA."[79] Therefore, if a user sets their content visibility to anything other than public, it qualifies as private. This was confirmed in *Ehling v. Monmouth-Ocean Hospital Service Corp.*, in which the District Court of New Jersey found that "when users ma[d]e their Facebook wall posts inaccessible to the general public, the wall posts [we]re 'configured to be private' for the purposes of the SCA."[80] Similarly, in *Facebook v. Superior Court (Hunter)*, the Supreme Court of California held that social media posts that were configured to be public fell within § 2702(b)(3)'s lawful consent exception, which allows ISPs to disclose a user's content with the user's consent.[81] By this logic, if a user's content is visible to the public, they are consenting to the RCS provider's disclosure of their content. The SCA, therefore, does not protect social media content that is posted publicly because consent is an exception to the prohibition of voluntary disclosure under § 2702. The *Hunter* court also held that "restricted communications sent to numerous recipients cannot be deemed to be public—and do not fall within the lawful consent exception."[82] In other words, even if social media communications are limited to a large group of people, that does not mean these posts are considered public. According to the *Ehling* court, "the critical inquiry is whether Facebook users took steps to limit access to the information . . . . Privacy protection provided by the SCA does not depend on the number of Facebook friends that a user has."[83] By restricting one's content with privacy settings, a social media user can therefore take advantage of the SCA's privacy protections and make it more

78. *See Facebook Privacy Basics*, FACEBOOK, https://www.facebook.com/about/basics/manage-your-privacy [https://perma.cc/NNR8-NFLX]; *Facebook Privacy Basics: Posts*, FACEBOOK, https://www.facebook.com/about/basics/manage-your-privacy/posts [https://perma.cc/6Y9P-8V73]; *Privacy Policy*, SNAPCHAT, https://snap.com/en-US/privacy/privacy-policy [https://perma.cc/J3RW-7NUS]; *Meta Privacy Center: Privacy Policy*, INSTAGRAM, https://privacycenter.instagram.com/policy [https://perma.cc/9THM-CLEX].

79. *Crispin*, 717 F. Supp. 2d at 981; *see also* Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 666 (D.N.J. 2013) ("Facebook wall posts fall within the purview of the SCA.").

80. *Ehling*, 961 F. Supp. 2d at 668.

81. Facebook, Inc. v. Superior Court (Hunter), 417 P.3d 725, 728 (Cal. 2018).

82. *Id.*

83. *Ehling*, 961 F. Supp. 2d at 668.

difficult for the government to obtain their content—by requiring them to get a warrant, for example—for use in a criminal case, but not all users are that savvy or careful.

Based on this jurisprudence, it should not matter how broad the user's privacy settings are—as long as the individual specifically took steps to limit who can view their content, it becomes protected from voluntary disclosure. This is not foolproof, however, because, as discussed earlier, disclosure may still be permitted if authorized by § 2703.[84] This remains problematic because, as Justice Sotomayor stated in *Jones*, a Fourth Amendment search online occurs when the government violates a "subjective expectation of privacy[,]"[85] and one could argue that when an individual invokes privacy settings, they reasonably expect that their content will be kept private. If obtaining individuals' social media data constitutes a search, then under Justice Roberts's logic in *Carpenter*, a warrant should be required because social media content can contain lots of information about a person's day, including their location and movements, like the cell site records in *Carpenter*. Therefore, it stands to reason that all searches of private social media content should require a warrant, which is not currently the case under the SCA.

2. Social Media: Does Disclosure of Its Content Follow ECS or RCS Regulations?

As previously discussed, the SCA has different standards for an ECS than for an RCS—the government can more easily obtain communications from an RCS, whereas obtaining communications from an ECS depends on how long ago the communications were created, thus emphasizing the importance of properly categorizing each social media platform. In *Crispin*, the court found that social media platforms can be characterized differently depending on the state of the messages: before the messages have been opened, ISPs operate as ECS providers, but once the messages have been opened and retained, the ISPs operate as RCS providers.[86] This creates significant complexity and results in variability in how the SCA is applied to each social media platform, given the different standards between RCS and ECS providers and the difficulty in determining which standard will apply.

The *Crispin* court acknowledged that Facebook wall posts and MySpace comments "present a distinct and more difficult question" as to

84. 18 U.S.C. § 2702(b)(2).

85. United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring) (citing Kyllo v. United States, 553 U.S. 27, 31–33 (2001)).

86. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010).

whether the social media platforms are acting as ECS or RCS providers.[87] On one hand, the court stated that Facebook and MySpace were ECS providers with respect to wall posts and comments because they were being held for "backup purposes once read."[88] Here, the court relied on *Snow v. DIRECTV, Inc.*, in which a district court found that because electronic bulletin board services ("BBS") did not have temporary, intermediate storage, they were actually storing the information for backup purposes and thus were an ECS.[89] The court analogized Facebook and MySpace wall posts and comments to BBS, concluding that these posts and comments were also being stored for backup purposes since they were not deleted after being read, and thus the social media platforms should be considered ECS providers.[90]

On the other hand, the court also said that Facebook and MySpace could be considered RCS providers with respect to wall posts and comments because they maintained these communications not only for storage, but also for display purposes, as users wanted their friends to be able to see the communications.[91] The court relied on *Viacom International Inc. v. YouTube Inc.* in this instance, analogizing Facebook wall posts and MySpace comments to private YouTube videos.[92] In *Viacom*, the court found that YouTube was an RCS provider because it stored videos on behalf of its subscribers.[93] Thus, the *Crispin* court concluded that Facebook wall posts and MySpace comments, like YouTube videos, can be stored for the purpose of allowing other users to view the content, thus making Facebook and MySpace RCS providers, like YouTube.[94] Ultimately, the court did not rule whether Facebook and MySpace were ECS or RCS providers with respect to wall posts and comments, remanding the case for further development.[95] This complexity demonstrates how ill-suited the SCA currently is to protect individuals' privacy on social media platforms, as there is no clear and consistent way to apply it. Further, the arguments made in *Crispin* emphasize just how arbitrary the distinction between an RCS and ECS provider can be when it comes to social media platforms. Because social media platforms do not fit neatly into either category, courts can come to different conclusions as to how these ISPs should be regulated, thus leading to uncertainty

87. *Id.* at 988.
88. *Id.* at 989.
89. *Id.* at 988 (citing Snow v. DIRECTV, Inc., No. 2:04-cv-515-FtM-33SPC, 2005 U.S. Dist. LEXIS 48652 (M.D. Fla. May 9, 2005)).
90. *Id.* at 989.
91. *Id.* at 990.
92. *Id.*
93. *See* Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008).
94. *Crispin*, 717 F. Supp. 2d at 990.
95. *Id.* at 991.

regarding the protection of privacy rights of social media users. This arbitrariness can be explained by the fact that the SCA was written in 1986, as articulated in *Konop v. Hawaiian Airlines, Inc.*:

> [T]he ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like [social media platforms]. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.[96]

The *Konop* court's words make clear that the SCA has become outdated because Congress was unable to foresee the problems that would arise for privacy protections resulting from not yet existing communication technologies. This is further supported by the fact that the *Crispin* court was unable to make a decision regarding the status of Facebook and MySpace with respect to wall posts and comments, given the limitations in clearly and consistently applying the SCA to communications on the various social media platforms.[97] Courts' inability to readily place certain features of social media platforms into existing categories highlights the inadequacy of the SCA in affording privacy rights to users of the prevalent modern technologies and supports that now is the time to change the SCA to clarify its applicability and afford stronger protections for various types of social media communications by creating more appropriate categories that these ISPs can be classified into.

3. Challenges in Applying SCA Content Disclosure to Stories

Stories are a relatively new feature of social media platforms, having only been in existence since 2013.[98] Like with the aforementioned difficulty in generally applying the SCA to social media platforms and user content, Stories, which disappear within twenty-four hours, provide another example that highlights the limited applicability of the current statutory framework under the SCA to modern communication technologies. From a privacy perspective, the good news is that most of these posts are removed from ISPs' servers as soon as the twenty-four hour period is up.[99] Since the content

96. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

97. *See* Christopher J. Borchert, Fernando M. Pinguelo & David Thaw, *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 56 (2015) ("The *Crispin* court's reasoning is both conflicted and irresolute, and thus fails to clarify the SCA's applicability to communications made via social networking platforms.").

98. Wiltshire, *supra* note 24.

99. *See What Happens to Content (Posts, Pictures) That I Delete from Facebook?*, FACEBOOK, https://www.facebook.com/help/121995105053180 [https://perma.cc/DR4U-RXPJ]; *Stories*, INSTAGRAM, https://help.instagram.com/1660923094227526 [https://perma.cc/8VFX-TH2V]; *When Does Snapchat Delete Snaps and Chats?*, SNAPCHAT, https://support.snapchat.com/en-US/article/when-are-snaps-chats-

is no longer on the social media platform's server, it is not possible for ISPs to disclose this content—even pursuant to a court order, subpoena, or warrant—because the content would no longer be in storage.[100] However, concerns remain for any content that remains saved on the server, which might still be obtainable for criminal investigations under the current SCA.

In addition, both Facebook and Instagram Stories can be saved in Story Archives,[101] and Snapchat Stories can be saved in Memories.[102] This content, therefore, could feasibly be disclosed to the government under the SCA if the proper exceptions and procedures were met. Because part of the appeal of Stories is that posts are only available for twenty-four hours, users likely do not think about how long their content is maintained in storage. Rather, many incorrectly assume that the content has been permanently deleted when the twenty-four hours expire. The problem here is that if Stories are governed by current ECS rules, once Stories are more than 180 days old, they can be obtained with notice and a subpoena or court order. This goes against the intent underlying Justice Robert's opinion in *Carpenter* because one could similarly argue that individuals who post Stories believe they have a reasonable expectation of privacy in these Stories that are now only available for their own view, yet they can, in fact, still be obtained with lesser protections than a warrant. Therefore, even though the SCA was intended to extend the protections of the Fourth Amendment to online communications, currently it does so unsuccessfully, particularly in the case of Stories.

Because Stories are so new, there have not been many cases addressing how the SCA applies to them. In *Facebook, Inc. v. Pepe*, the District of Columbia Court of Appeals considered an allegedly sent "disappearing Instagram 'Story' " for the first time. [103] The court found that the Instagram

deleted [https://perma.cc/2JF3-MJQG].

100. *See* Ian Hoppe, *Does Law Enforcement Have Access to Your Snapchat Photos? A Simple Guide*, AL.COM (Jan. 13, 2019, 8:19 PM), https://www.al.com/business/2014/11/snapchat_subpeona.html [https://perma.cc/47K9-WJDP] ("Snapchat will not turn over the content of your past Snapchats because it no longer has access to them. Snapchat couldn't cooperate with law enforcement even if they wanted to, because, as part of their base operations, the content of messages is not available to them.").

101. Facebook Stories are "only available to [the] selected audience for 24 hours, but after that they can be saved in [the] story archive." *View Your Facebook Story Archive*, FACEBOOK, https://www.facebook.com/help/2241356632587629 [https://perma.cc/25Q3-WL7U]. By saving Facebook Stories to the Story Archive, users can still view their stories even though they are no longer visible to anyone else. Users can turn their Story Archive on or off, though Facebook does not specify what happens to Stories when the archive is turned off. Similarly, Instagram Stories are automatically saved to the Stories Archive unless this setting is turned off. *Stories*, *supra* note 99.

102. Snapchat contains a feature called Memories, which is backed up by Snapchat, that allows users to save Snaps and Stories so that they can be looked back on anytime. Snapchat Support, *supra* note 99. Therefore, although "Snapchat servers are designed to automatically delete all Snaps after they've been viewed by all recipients," users can still elect to save this content on Snapchats servers. *Id.*

103. Facebook, Inc. v. Pepe, 241 A.3d 248, 252 (D.C. 2020).

Story was content under the SCA, and that because James Pepe was an "addressee or intended recipient" under § 2702(b), Facebook was permitted to disclose any Instagram Stories that were responsive to the subpoena.[104] However, this addressee or intended recipient exception would not apply if the government were seeking disclosure in a criminal case, as the individual who posted the Story would likely not have invited a government official to view their private Facebook, Instagram, or Snapchat Story. Thus, the inquiry then shifts to consider whether social media platforms are acting as RCS or ECS providers when it comes to Stories.

One could analogize Stories to Facebook wall posts and MySpace comments when applying the SCA to social media Stories. Following the *Crispin* court, this would mean that ISPs offering Stories could be considered either RSC or ECS providers. The first argument is that Facebook, Instagram, and Snapchat act as ECS providers when individuals post Stories because the individual is "sending" the electronic communication to the people who they have allowed to view it.[105] This would follow from analogizing Stories to wall posts or comments that are in "backup" storage. As per *Crispin*, if the messages are being stored on the servers solely because they were not deleted, then they are in backup storage and, thus, should be governed by ECS rules. Unfortunately, users do not usually think about deleting this type of content because they know that once it disappears, no one else can see it. However, what they often fail to realize is that these communications are then considered to be in backup storage, meaning they can still be disclosed to the government under the SCA.

Alternatively, Facebook, Instagram, and Snapchat could be considered RCS providers because they are simply storing the Stories on the server for others to view.[106] In *Crispin*, wall posts were compared to YouTube videos that were stored for the purpose of allowing other users to view the content.[107] Arguably, Stories are also stored for the purpose of allowing others to view them, not simply because they have not been deleted. Therefore, even though a Story disappears after twenty-four hours, the user can reshare the content from their Archive, similar to changing a YouTube video's settings to modify who can view it at any point in time.

On the other hand, Stories could also be analogized to private messages, which further complicates the analysis of SCA protections, particularly when considering the reasoning in *Crispin*, which stated that when a message is

104. *Id.* at 256.
105. *See* 18 U.S.C. § 2510(15).
106. *See id.* § 2711(2).
107. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 990 (C.D. Cal. 2010).

unread, the ISP acts as an ECS, but once the message has been read, the ISP then acts as an RCS.[108] Stories can be viewed by whomever the user allows, depending on their privacy settings, meaning that at any given point in time, the Story might have been viewed by a portion, but not all, of the potential audience. Thus, is the Story considered "unread" until all possible viewers have seen it, or does it switch to being "read" once at least one individual has viewed it? Alternatively, a Story could be "sent" while it is available for viewing by others but then switched to "read" once the twenty-four hours are up.

Whether or not a Story is considered to be an ECS or an RCS function directly impacts how law enforcement agencies can obtain its contents since the content of a Story would only be protected with a warrant if it were governed by ECS rules and 180 days old or less. Otherwise, Stories could be obtained with either a subpoena or a court order, making them easier to acquire for criminal investigations. These types of questions have not yet been adequately addressed by courts, and because Stories have qualities of both RCS and ECS communications, it is not possible to consistently predict whether RCS or ECS rules should govern in individual cases. The difficulty in determining how to appropriately apply the SCA to Stories supports the need for the proposed changes to the SCA.

### B. OBTAINING NON-CONTENT DATA FROM SOCIAL MEDIA POSTS

#### 1. Applying SCA Non-Content Disclosure to Social Media Platforms

Disclosure of non-content data stored by social media platforms is different from disclosure of content in that non-content disclosure does not depend on whether the provider is an ECS or an RCS. While content is defined as including "any information concerning the substance, purport, or meaning of that communication,"[109] non-content is not well-defined. The SCA does, however, define some non-content data that can be obtained with only a subpoena, including the user's name, address, and telephone number.[110] This stems from the third-party doctrine, which states "the Fourth Amendment does not prohibit the [government from] obtaining . . . information revealed to a third party."[111] This creates an exception to the reasonable expectation of privacy that is protected by the

108. *Id.* at 987.
109. 18 U.S.C. § 2510(8).
110. *See id.* § 2703(c)(2).
111. United States v. Miller, 425 U.S. 435, 443 (1976) (holding that a defendant had no expectation of privacy in his bank records because he had disclosed his affairs to his bank when opening his accounts); *see also* Smith v. Maryland, 442 U.S. 735, 745 (1979) (holding that a defendant had no actual expectation of privacy in the phone numbers he dialed and that even if he did, the expectation was not reasonable).

Fourth Amendment: once an individual voluntarily shares information with a third party, they lose any reasonable expectation of privacy in that information.[112] It can be assumed, however, that non-content data is any information that is not the main substance of the communication, including the metadata incorporated in the communication, for example, the user's identity, location, payment information, and telephone number.[113] This is problematic because under § 2703(c), non-content data can sometimes be easily obtained by the government with a court order. Because the SCA does not explicitly state which types of non-content data can be obtained with a court order and which require a warrant, a lot of discretion is left to police officers and the courts.

"Some non-content information, particularly associational information and location information, is inherently expressive, capable of directly exposing intimate details of an individual's life."[114] In the age of social media, people are constantly posting images and videos online;[115] when people take photos, for example, the image files contain metadata that includes the time and date when the image was taken, along with the exact location where the photograph was taken.[116] Facebook, Instagram, and Snapchat collect a lot of information about an individual's daily life, including sensitive location information.[117] Like wireless providers, Facebook, Instagram, and Snapchat are all able to collect individuals' locations from Bluetooth signals, wireless networks, and cell towers.[118] Additionally, these platforms also store information such as the location,

112. *Miller*, 425 U.S. at 443.

113. "One approach to distinguishing content from non-content is to divide electronic communications into 'payload' (content) and 'delivery instructions' (non-content)." Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond the Content/Non-Content Distinction*, 54 SANTA CLARA L. REV. 821, 830 (2015) (arguing that information such as the IP address from which a comment on social media is posted is non-content).

114. *Id.* at 831.

115. On Instagram alone, "[a]t least 95 million photos and videos are posted . . . each day." Jack Flynn, *30+ Instagram Statistics [2022]: Facts About This Important Marketing Platform*, ZIPPIA (May 23, 2022), https://www.zippia.com/advice/instagram-statistics [https://perma.cc/ZCH2-FZ4S].

116. Gurpreet Singh, *Understanding Metadata for Photographers*, PIXPA (June 23, 2020), https://www.pixpa.com/blog/photo-metadata [https://perma.cc/273F-GNJT].

117. *Meta Privacy Center: Privacy Policy*, META (July 26, 2022), https://www.facebook.com/privacy [https://perma.cc/N48L-2EM4] (describing data policies for Facebook and Instagram); *Privacy Policy*, *supra* note 78. As of October 2021, Facebook Inc., the company that owns both Facebook and Instagram, changed its name to Meta. Mike Isaac, *Facebook Renames Itself Meta*, N.Y. TIMES (Nov. 10, 2021), https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html [https://perma.cc/WUD4-KFLH]. Thus, the Meta Privacy Policy details the information collected by both Facebook and Instagram. *See* Michel Protti, *Here's What You Need to Know About Our Updated Privacy Policy and Terms of Service*, META (May 26, 2022), https://about.fb.com/news/2022/05/metas-updated-privacy-policy [https://perma.cc/YW5H-4A2F] ("The updated Meta Privacy Policy covers Facebook, Instagram, Messenger and other Meta products.").

118. *See Meta Privacy Center: Privacy Policy*, *supra* note 117; *Privacy Policy*, *supra* note 78.

date, and time at which the photograph or file was created.[119] This information could be used in a criminal investigation to pinpoint the time and place where a crime occurred or where a suspect was located at a particular time, making it highly valuable for the government when charging someone with a crime.[120] Thus, it is important to afford this information the highest level of protection.

Because social media is a newer phenomenon, most courts have yet to address the issue of obtaining non-content data, which can include time and location information from a social media platform. In *In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, a magistrate judge ordered Twitter[121] to turn over information pertaining to multiple subscribers; this information included "records of user activity . . . including the date [and] time" as well as "non-content information associated with the contents of any communication . . . [including] IP addresses."[122] The Virginia district court held that because § 2703(d) requires the government to show only "reasonable grounds" that the records sought are relevant and material to an ongoing criminal investigation, and because the third-party doctrine applies to IP address information, the court order was valid.[123] The court differentiated IP addresses from beeper monitoring because IP addresses are shared with all internet routers when a user accesses Twitter, while tracking a beeper allowed the government to monitor inside a private residence, which was not otherwise open for visual surveillance.[124] While this case clarified what one district court believed the SCA means for IP addresses, it does not help to clarify how the SCA applies to exact location information such as the metadata embedded in Facebook, Instagram, and Snapchat posts.

However, courts have addressed the issue of whether obtaining location

119. *See Meta Privacy Center: Privacy Policy*, *supra* note 117; *Privacy Policy*, *supra* note 78.

120. In *United States v. Hart*, the court held that "any expectation of privacy a person might have had in non-communication records given to a third party is destroyed upon disclosure, even if he disclosed the information on the assumption that it would be used only for a limited purpose." United States v. Hart, No. 3:08-CR-00109-C, 2009 U.S. Dist. LEXIS 72597, at *45 (W.D. Ky. July 28, 2009). However, the non-content information that the government obtained included login tracker data, such as the date and time of the user's last log in, and the user's IP address, which allowed it to determine the exact location from which the email was sent. *Id.* at *13. This is troubling because it means that the government can easily obtain non-content information without a warrant and track a defendant's precise location, which would reasonably require a warrant otherwise.

121. Twitter is a social media platform that allows individuals to communicate with family, friends, and the general public through "Tweets," which can be comprised of text, photos, and videos. *See New User FAQ*, TWITTER, https://help.twitter.com/en/resources/new-user-faq [https://perma.cc/DZE7-JMCE] (describing how Twitter works).

122. *In re* Application of the U.S. for an Ord. Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 121–22, 130–31, 153 (E.D. Va. 2011).

123. *Id.* at 121–22.

124. *Id.* at 132.

information from a wireless carrier constitutes a search under the Fourth Amendment. In *Carpenter*, the Court held that a court order obtained under § 2703(d) was not a permissible means of acquiring a defendant's historical cell-site location information ("CSLI") from a wireless carrier.[125] The Court found that individuals have a reasonable expectation of privacy in their physical location, and when the government accessed CSLI from the wireless carriers, it violated the defendant's reasonable expectation of privacy.[126] As a result, the Court held that the government "must generally obtain a warrant supported by probable cause" before acquiring records containing location information.[127]

Because the SCA was intended to extend Fourth Amendment rights to online communications, it might be acceptable to infer that obtaining location information from social media platforms would also require obtaining a warrant supported by probable cause. However, the *Carpenter* Court articulated that its decision was "narrow" and that it does not "address other business records that might incidentally reveal location information,"[128] which means that the metadata contained in the photos and videos posted on social media may not require the government to obtain a warrant, which could compromise people's privacy rights. As Justice Sotomayor pointed out in her concurrence in *Jones*, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy" in the information they disclose online.[129] "This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[130] Justice Sotomayor is right: in the digital age, individuals post a wealth of information online that they expect—as a result of their privacy settings—to be visible only to those they choose. Thus, it is time to reconsider the notion that revealing this information to third-party social media platforms means that the government should be able to easily obtain their locational information because there is no "reasonable expectation of privacy."[131]

2. Challenges in Applying SCA Non-Content Data Disclosure to Stories

Stories provide users with the unique opportunity to create information that can qualify as both content and non-content data at the same time. When

125. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).
126. *Id.* at 2217–19.
127. *Id.* at 2221.
128. *Id.* at 2220.
129. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).
130. *Id.*
131. *Id.*

an individual posts their Story online, they are able to add "stickers," which can indicate to those viewing the Story the exact location of the individual and the date and time the Story was posted, among other things. Thus, when a user posts a location in their social media Story, it actually appears as part of a graphic. In this sense, it would appear to be content because it is part of the image. On the other hand, since it is a location, Instagram will likely also collect that information separately from the content. It would then appear that, in this situation, the location information would be both content and non-content data at the same time; how then should a court determine whether a subpoena, court order, or warrant is required to compel the information from Instagram? Unfortunately, this is unclear under the current statutory framework of the SCA.

Former CIA agent Michael Morell admits that "[t]here's a lot of content in metadata" and that "[t]here's not a sharp difference between metadata and content . . . It's more of a continuum."[132] If even the government accepts that it is difficult to distinguish between content and non-content data, then the SCA should not be differentiating between the two and allowing weaker protections for non-content data when, in fact, it may reveal information just as sensitive as content. Because the SCA was created prior to the creation of social media, it does not account for the overlap in the types of information that can be obtained from non-content and content data. This is another reason why the SCA needs to be rewritten: to clarify and remove the ambiguity of how sensitive non-content information can be disclosed.

## V. REVISING THE STORED COMMUNICATIONS ACT

### A. REQUIRING WARRANTS FOR ALL COMPELLED CONTENT DISCLOSURES

While the SCA provides some protections for private communications on ISPs, the statute needs to be updated and better tailored so that it is applicable to all the various nuances of modern technologies. Currently, the strongest protections are afforded to unretrieved emails and other temporarily stored files that are 180 days old or less.[133] All other communications can be more easily obtained with a subpoena combined with prior notice.[134] Under the Federal Rules of Criminal Procedure, a subpoena "may order the witness to produce any books, papers, documents, data, or

132. Julian Sanchez, *Obama Backs Off Real NSA Reform*, DAILY BEAST (Apr. 14, 2017, 1:04 PM), https://www.thedailybeast.com/obama-backs-off-real-nsa-reform [https://perma.cc/2XQT-DZY4] (quoting Michael Morell).

133. 18 U.S.C. § 2703(a); *see also* Kerr, *supra* note 68, at 1233 (identifying that only transmissions pending for 180 days or less "receive the protection of a full warrant requirement").

134. 18 U.S.C. § 2703(a), (b)(1)(B).

other objects the subpoena designates."[135] This is even less protective of an individual's right to privacy than having to obtain a court order, which requires that the "governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a[n] . . . electronic communication . . . are relevant and material to an ongoing criminal investigation."[136] To obtain a warrant, on the other hand, there must be "probable cause to search for and seize a person or property."[137] This places a heavier burden on the government and thus ensures that social media users are not losing their right to privacy without stringent protections, which should be the goal of any such legislation.

Because the line between defining a social media platform as either an ECS provider or an RCS provider is so unclear, applying existing laws can lead to variable results that negatively impact users' privacy rights. As previously discussed, under the SCA, the same ISP can be treated as an ECS for some functions, but an RCS for others; this leaves users with inconsistencies in the treatment of their personal communications, which can infringe on their privacy. Importantly, whether a social media platform is characterized as an ECS or an RCS has a direct impact on the stringency of the procedures that law enforcement must follow to obtain the content. Further, although the SCA does not specifically differentiate between public and private social media accounts, because the SCA was only intended to cover private communications, it inadvertently creates counterintuitive privacy protections. For example, in *Crispin*, the court held that opened private messages on Facebook and MySpace were covered by RCS rules, while ECS rules covered restricted wall posts and comments.[138] Effectively, this meant that wall posts and comments, which can arguably be seen by all of an individual user's friends, were afforded greater protections than private messages, which are typically only seen by the sender and the intended recipient. This is counterintuitive because it means that less private communications receive greater protection than more private communications.

Consequently, there is a clear need for Congress to reform the SCA now, and as a first step, require warrants for all communications, regardless of whether an ISP is characterized as an RCS or ECS.[139] Warrants provide

135. FED. R. CRIM. P. 17(c)(1).
136. 18 U.S.C. § 2703(d).
137. FED. R. CRIM. P. 41(d)(1).
138. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).
139. In April 2022, the Warrant for Metadata Act was introduced in the House of Representatives, proposing that warrants be required for ECS and RCS disclosures. Warrant for Metadata Act, H.R. 7553, 117th Cong. (2022). Thus, it is clear that at least part of Congress has recognized the need for tighter restrictions to protect the liberties of U.S. citizens; only time will tell if this bill will pass and the SCA

the strongest protection for social media users, and when it comes to individual liberties, the government has an obligation to preserve these liberties with the broadest legal protections possible.[140] This is especially important considering the case law, which argues that individuals have a right to be protected under the SCA if they took steps to protect their content.[141] By requiring warrants for the disclosure of all social media communications, the SCA would be able to provide the strongest statutory framework to protect users' privacy and prevent the unjust use of their social media content against them in criminal court.

### B. REMOVING THE DIFFERENTIATION BETWEEN RCS AND ECS

The previously highlighted variability and liability in characterizing social media platforms as RCS providers in some instances and ECS providers in others has become even more problematic with the recent emergence of social media Stories. If Stories are analogized to emails or private messages—because the user posts the Story with the intention that others will see it and it will be gone shortly after the message is read—they would be governed by ECS rules, similar to the private messages in *Crispin*.[142] Alternatively, Stories considered analogous to YouTube videos—because they are stored for only a limited number of people to view—would be governed by RCS rules.[143] The courts have yet to address whether Stories should be governed by ECS or RCS rules, but there are arguments for both sides because Stories do not fit neatly into either category.

Because the SCA was not created to accommodate these newer technologies, it would be more effective to revise the SCA categories rather than attempting to fit new technologies into the existing categories. Because social media platforms offer various functions that involve both message

will finally be amended, as amendments have been proposed before with no success. *See, e.g.*, Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2013); Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (2013); Electronic Communications Privacy Act Amendments Act of 2015, S. 356, 114th Cong. (2015); Email Privacy Act, H.R. 699, 114th Cong. (2016).

140. "No person shall be . . . deprived of life, liberty, or property, without due process of law . . . ." U.S. CONST. amend. V. A citizen's right to liberty is derived from the U.S. Constitution, which means that while the "[g]overnment has an obligation to protect the safety and security of its citizens, . . . it has an equally important responsibility to safeguard the freedoms and liberties that are the cornerstones of American democracy." Anthony D. Romero, *In Defense of Liberty at a Time of National Emergency*, ABA: HUM. RTS. MAG. (Jan. 1, 2002), https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/human_rights_vol29_2002/winter2002/irr_hr_winter02_romero [https://perma.cc/9AUZ-CY8D].

141. Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 668 (D.N.J. 2013).

142. *Crispin*, 717 F. Supp. 2d at 980.

143. Viacom Int'l, Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008).

transmissions and electronic storage, the language of the SCA needs to be amended to eliminate the distinction between RCS and ECS altogether. Orin Kerr suggested doing this by identifying that the SCA applies only to "network service providers," which would encapsulate the current definitions of ECS and RCS and then apply the SCA rules to different types of files held by the network service providers.[144] This would alleviate the difficulty of determining which rules apply to social media providers in different situations and would further clarify privacy rights for users by establishing when and how their content is protected. Importantly, this would also provide consistency and give users a better understanding of their rights online, which may, in turn, influence what information they choose to post on social media—especially if they know it could later be used against them in a criminal case. Without this clarity, social media users do not know whether their content is protected and what steps they need to take to protect their private communications, which may, consequently, have a "chilling effect"[145] on their conduct.

### C. REQUIRING WARRANTS FOR ALL COMPELLED NON-CONTENT DATA DISCLOSURES

As technology has grown and evolved, the distinction between content and non-content data has continued to blur. This is particularly true when individuals include the date, time, and location of their posts in the actual post or Story. When Facebook, Instagram, and Snapchat collect that information, it becomes non-content data, some of which can be disclosed pursuant to only a subpoena, and some of which requires either a court order or a warrant. One way to address this issue would be to require warrants for all compelled disclosures of non-content data. This is in line with the suggestion to require warrants for all compelled disclosures of content.

By requiring warrants for compelled disclosures of non-content data, criminal investigators would then have to show probable cause before obtaining the information, which is the highest standard available. In *Carpenter*, the Court acknowledged that individuals have a reasonable expectation of privacy regarding their physical location.[146] Unlike cell-site records, social media platforms do not collect information on users every time their phone pings a cell tower. Instead, locations are collected when

144. Kerr, *supra* note 68, at 1235.

145. A chilling effect is "[t]he result of a law or practice that seriously discourages the exercise of a constitutional right." *Chilling Effect*, Black's Law Dictionary (11th ed. 2019). The constitutional right affected here would be the freedom of speech, as social media users are expressing the right to speak freely when they post content online.

146. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

individuals post to social media. Therefore, it is currently unclear whether location information would always be protected by a warrant under the SCA.[147]

While it is true that some non-content data records reveal more than others, advances in metadata analysis have shown that assembling disparate pieces of metadata can lead to larger discoveries. Thus, although one might argue that it would be better to specify which types of records require a subpoena, which require a court order, and which require a warrant, this practice would be difficult to consistently implement.[148] Rewriting the SCA to guarantee that such non-content metadata is protected by the highest protection affordable would ensure that social media users are provided their First Amendment rights.

### D. REMOVING THE DISTINCTION BETWEEN CONTENT AND NON-CONTENT DATA

Perhaps a simpler solution to this problem of differentiating between content and non-content data would be to eliminate the distinction altogether. The distinction comes from *Ex parte Jackson*, in which the Court held that "a distinction is to be made between different kinds of mail matter,—between what is intended to be kept free from inspection, such as letters . . . and what is open to inspection, such as . . . printed matter, purposely left in a condition to be examined."[149] The Court held that mail can only be opened and examined under a warrant because otherwise it would constitute an illegal search.[150] Thus, content is what is "intended to be kept free from inspection," as it is sealed away, and non-content data is what is left in the open.

When the Court first created this distinction in *Ex parte Jackson*, it made sense to differentiate between the information on the outside of an

147. In 2013, the 113th Congress proposed the Online Communications and Geolocation Protection Act. This proposed amendment to the SCA included prohibitions on the disclosure of geolocation information to governmental entities. Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2013); *see also* Dell Cameron, *New Bill Would Halt Warrantless Requests for Consumers' Geolocation Data*, DAILY DOT (May 29, 2021, 3:18 PM), https://www.dailydot.com/debug/online-communications-geolocation-protection-act [https://perma.cc/V8BT-B3S3] (stating that the lawmakers said that "the ECPA in its current form offers inadequate protections to Americans who rely heavily on mobile devices operating location-based services"). Thus, Congress is aware that the SCA does not adequately protect against disclosure of non-contents containing location information. Although the bill was proposed, it was never passed and thus the problem remains.

148. *See* Kerr, *supra* note 12, at 413 ("Identifying the proper particularity standard for noncontent information is difficult because such records exist in many different forms . . . . A list of every email address that a person emailed, together with the time each email was sent, is more sensitive than merely the name on the account.").

149. *Ex parte* Jackson, 96 U.S. 727, 733 (1878).

150. *Id.*

envelope, which could be openly seen by others, and the content that was stored within an envelope. However, trying to apply that logic to social media now no longer makes sense because the distinction between content and non-content data has become so blurred. For example, when a user posts a picture of their dog on their Instagram profile, they can include a geotagged location to where the photograph was taken. Is the location still non-content data because it is not the "substance" of the post, or is the location content because the user is using it to indicate where the picture was taken and, therefore, it is part of the description? If the latter were true, it would then arguably be content.

If the same information can be considered both content and non-content, it does not make sense to allow law enforcement to obtain the same information with lesser protections solely because they can argue that it is non-content data. Eliminating the distinction between non-content and content data would remove the uncertainty and enable social media users to be confident that all aspects of their posts would be protected.

## CONCLUSION

The Ninth Circuit had it right when it said, "until Congress brings the laws in line with modern technology, protection of the Internet and websites such as [social media platforms] will remain a confusing and uncertain area of the law."[151] Social media platforms, as a whole, do not fit nicely into the existing ECS and RCS categories that Congress created when drafting the SCA in 1986. Some functions of social media platforms lead to the platform being treated as an ECS, while other functions lead to the platform being treated as an RCS. In other instances, it is difficult to determine whether a specific function indicates that the social media platform is acting as an ECS or an RCS. As a result, the SCA can be inconsistently applied to disclosures of social media content. Most importantly, certain functions on social media are arbitrarily afforded stricter protections than others, solely because of how they are inconsistently categorized under the current SCA. The rationale for affording communications greater protections when they are classified as an ECS that is 180 days old or less versus the fewer protections afforded to an ECS that is more than 180 days old or as an RCS is unclear. As a result of these arbitrary distinctions, law enforcement has an easier time searching an individual's private social media, which may only require a subpoena or court order, than it would going through someone's diary, which requires a warrant.

Further complicating the application of the SCA to social media today

151. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

is the fact that in the age of social media, it is becoming more difficult to distinguish content from non-content data. When Congress drafted the SCA, it attempted to apply the Fourth Amendment to online communications and therefore made a distinction between content and non-content data; however, the difference between what constitutes content—analogous to what is contained inside an envelope—and non-content—analogous to what is on the outside of an envelope—in the digital context has become difficult to discern.[152] Courts have also considered the third-party doctrine when determining what information could be obtained with a subpoena, reasoning that because the information had been disclosed to a third party, the user had no reasonable expectation of privacy. However, social media users disclose a variety of personal information when signing up for an account, often including, at a minimum, their name, birthdate, and email address, and their posts include lots of additional metadata. The privacy of these data is critical to define because they can be used by law enforcement to piece together where an individual was at the time they posted to social media or where an individual was when the content they posted was retrieved. Whether this very sensitive information should require a warrant or a lesser means to be retrieved by law enforcement is not currently clearly defined in the SCA.

The ECPA—which includes the SCA—was enacted to protect citizens from having their electronic communications intercepted without the proper authorization, but these protections need to change in response to evolving communication technologies. This legislation was intended to extend Fourth Amendment protections to new technologies, but because social media technologies have evolved so rapidly since 1986, the SCA no longer truly affords the intended protections. For citizens to be protected against unreasonable searches of their digital media, Congress needs to restructure the existing legislation to properly address how communication technologies have evolved over the past thirty-six years. Not only can one social media platform function as both an ECS and an RCS provider under the current SCA definitions, but it is now also difficult to determine whether a specific social media function, such as Stories, which has properties of both, should be governed by ECS or RCS rules. Further, there is now duplication of content and non-content data, making it difficult to clearly differentiate them and ensure that all of this personal information is being adequately protected under the SCA.

To ensure the protection of constitutional privacy rights and prevent private social media communications from being unfairly used against their creators in court, Congress should require that all compelled disclosures be governed

152. *See Ex parte* Jackson, 96 U.S. 727, 733 (1878).

by the same rules as the Fourth Amendment; that is, it should require that there be a warrant and "probable cause."[153] If all compelled disclosures were to require a warrant, then equal protections would be applied in all situations, as the standard would be consistent across physical and digital searches; this would help ensure that defendants' due process rights were not violated. Further, because the distinctions between an ECS and RCS, as well as content and non-content data, are no longer appropriate, it would be advantageous for Congress to revise the SCA to better align with modern technologies by drawing the necessary delineations based on the functions being used, not on the specific type of provider. This way, the SCA would not only better apply to modern technology, but it would hopefully also better apply to future emerging technologies.

153. U.S. CONST. amend. IV.