A NEW SCA FRAMEWORK TO UNCLOTHE THE BUSINESS MODEL ATTACK

Meet Mehta†

I. INTRODUCTION

The Stored Communications Act (SCA) is one of the main statutory structures protecting user communications in the online realm. The SCA prevents specific types of online service providers from voluntarily disclosing their subscribers' communications or being compelled to do so, except in very limited circumstances.[1] As online services have steadily grown, becoming essential and ever-prevalent aspects of our daily lives, so has the importance of the SCA. Today, with many of our communications and interactions happening over social media and other online services, it is essential that the SCA is there to protect our information.

Although the importance of the SCA to protecting user privacy is evident, courts have often found it difficult to apply to modern services and technologies.[2] The SCA was enacted in 1986, before the arrival of the modern internet, and is thus severely outdated. It relies on simplistic service classifications (i.e., communication services vs. storage services) that no longer apply in order to create a hierarchy of communication protections. Courts have therefore "struggled to analyze problems involving modern technology within the confines of [the SCA] framework" and have called on Congress to update the SCA.[3] The SCA, however, has not yet been updated, leaving judges to wade through a "confusing and uncertain area of the law."[4]

Perhaps due to the fact that courts have found it frustrating to apply the SCA to modern technologies, courts and, to a large extent, the legal community as a whole, have often operated under the premise that social media companies are regulated by the SCA.[5] This assumption, however, was most recently challenged in *Facebook v. Superior Court*, in which a criminal defendant seeking

DOI: https://doi.org/10.15779/Z38FT8DK74

† J.D. 2022, University of California, Berkeley, School of Law.

[1] *See* 18 U.S.C. §§ 2702–03.

[2] *See* Facebook, Inc. v. Superior Ct. of San Diego Cnty., 471 P.3d 383, 406–07 (Cal. 2020) (Cantil-Sakauye, C.J., concurring).

[3] *Id.* at 407 (quoting Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002)).

[4] *See id.* (quoting *Konop*, 302 F.3d at 874).

[5] *See id.* at 412 (Cuéllar, J., concurring).

to subpoena Facebook claimed that Facebook did not qualify for the SCA's disclosure protections.[6]

In *Facebook*, the defendant advanced the business model theory, which argues that a company's business model of mining, analyzing, and sharing user content with third parties to facilitate targeted advertisements places the company outside of the disclosure provisions of the SCA.[7] According to the defendant, Facebook used such a business model and therefore contravened the SCA's explicit prohibition against the voluntary disclosure of user communications.[8] Thus, the defendant argued, Facebook could not use the SCA as a shield to protect itself from complying with a subpoena requesting user communications.[9] Though the court noted the potential importance of the business model theory and recognized that it deserved greater exploration, it did not adjudicate the issue; instead, it disposed of the case on other grounds.[10]

A deeper look in this Note, however, reveals that the business model theory is an impotent attack on social media services. Due to the communicative nature of social media and the industry trend of using advertisement-based business models that neither sell user information nor analyze user communications,[11] the business model attack falls flat: that is, it does not effectively change the application of the SCA's disclosure protections. Nonetheless, due to the sheer number of different social media services and business models available, courts should still implement business model scrutiny and engage in a fact-specific, case-by-case analysis when determining the exact scope of a particular service's SCA protections. Specifically, courts should analyze a service's business model as one step in a three-step analytical framework to help shape their analysis and solidify their reasoning.

Part II of this Note describes and provides background on the SCA. With that understanding in place, Part III discusses *Facebook v. Superior Court*, with a

[6] *See id.* at 402 (majority opinion).

[7] *See id.*

[8] *See id.* at 402–03.

[9] *See id.*

[10] *See id.* ("We conclude that the trial court below abused its discretion when ruling on the motion to quash by failing to apply the [applicable] test. . . . We will not assess the underlying merits of the business model thesis.").

[11] *See* Alfred Ng, *What Does it Actually Mean When a Company Says, 'We Do Not Sell Your Data"?*, THE MARKUP (Sept. 2, 2021), https://themarkup.org/the-breakdown/2021/09/02/what-does-it-actually-mean-when-a-company-says-we-do-not-sell-your-data [https://perma.cc/LU6J-3K7X]; *infra* note 169 and accompanying text.

special emphasis on Chief Justice Cantil-Sakauye's concurrence, where she quickly explores the business model theory.

Part IV begins with a short analysis and critique of Chief Justice Cantil-Sakauye's concurrence. Then, Part IV argues for a new three-step analytical framework for scrutinizing online and social media services under the SCA. The three steps consist of: (1) classifying the service as a communication or storage service; (2) determining whether the service authorizes access to user data, and if so, for what reasons; and (3) determining whether the business model or the service's interaction with user data limits the service's SCA protections. This analytical framework is meant to serve as a structuring tool, guiding courts away from improvised and ad-hoc analysis to a systematic method of analyzing modern services under the SCA.

After outlining the three-step analytical approach, Part IV then gives examples of putting that framework into practice. Part IV uses the proposed framework on three social media/web services: Gmail, Facebook Messenger, and Facebook Wallposts.

Finally, Part IV extrapolates from these examples and the business models of popular social media services to reach a final conclusion: the business model theory will be largely unsuccessful in attacking SCA disclosure protections provided to social media services. As the SCA stringently protects communication services, and as social media services are inherently communicative and are increasingly neither sharing nor analyzing their users' communications, the business model theory will not have a noticeable effect on SCA protections for social media sites.

II. A BACKGROUND OF THE SCA

In order to understand the impact of the business model theory on social media companies' disclosure protections under the SCA, it is important to first understand what the SCA is, why it was passed, and how it presents difficulties to courts in the modern world. By limiting specified entities from divulging their users' online and electronic communications, the SCA extends Fourth Amendment-like privacy protections in the online and digital realms. Although protecting online privacy is an ever-growing concern, because the SCA was enacted prior to the advent of the modern internet, courts sometimes find it difficult to apply the SCA to modern technologies and services.

A. THE STORED COMMUNICATIONS ACT

The SCA is a federal statute that governs how and when a service provider can disclose, either voluntarily or compulsorily, stored wired and electronic communications.[12] Enacted in 1986 as part of the broader Electronic Communications Privacy Act (ECPA), the SCA serves to "represent[] a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."[13] As the main statutory and legal framework protecting communications and subscriber information stored by online service providers (OSPs), the SCA plays a vital role in safeguarding Americans' online privacy interests. However, as the SCA was "written prior to the advent of the [modern] Internet," and has not been meaningfully updated, "the . . . statutory framework is ill-suited to address modern forms of communication."[14] Therefore, courts are often frustrated as they "struggle[] to analyze problems involving modern technology within the confines" of the statute.[15]

1. *The Purpose of the Stored Communications Act*

Congress enacted the SCA to extend privacy protections to electronic and internet communications that were largely left unprotected by the Fourth Amendment and the Wiretap Act of 1968.[16] The Fourth Amendment protects people from the government's arbitrary intrusions into their "houses, papers, and effects";[17] a person using the Internet, however, "does not have a physical 'home,' nor really any private space at all."[18] The Wiretap Act, on the other hand, addressed the unauthorized aural interception of "conversations using 'hard' telephone lines, but did not apply to interception of computer and other digital and electronic communications."[19]

The Fourth Amendment's third-party doctrine raised further doubts as to whether online communications would be protected. When accessing internet services, a user divulges their communications to multiple third parties. First, a user must connect to an internet service provider (ISP), such as Comcast or Verizon. The ISP then connects the user to the requested online service provider and acts as an intermediary for all communications to and from that service. Further, when a person uses an OSP, such as an email or online messaging service, the OSP will often keep a record of the user's communications for system integrity and user convenience. As such, online

[12] *See* 18 U.S.C. § 2702.

[13] H.R. REP. NO. 99-647, at 19 (1986).

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

[15] *Id.*

[16] *See* S. REP. NO. 99-541, at 2–3 (1986).

[17] U.S. CONST. amend. IV.

[18] 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 (2004).

[19] *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–23*, BUREAU OF JUST. ASSISTANCE, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 [https://perma.cc/G3CV-QYQM].

communications are often disclosed to (at least) two third parties, the ISP and the OSP, "that hold and process a user's information on the user's behalf."[20] As of 1986, however, the Supreme Court had regularly upheld the third-party doctrine, which states that there is no reasonable expectation of privacy for information divulged to third parties; consequently, no Fourth Amendment protection applies to that information.[21] In 1986, there was uncertainty over what extent, or if at all, the Fourth Amendment would protect computer and online communications.[22]

Congress emphasized these statutory and constitutional gaps when describing the purpose and necessity of the SCA and ECPA:[23] "This gap results in legal uncertainty. . . . Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right."[24]

The actual text of the SCA reveals another important goal of the statute: to provide privacy protections for electronic information *proportionate* to the privacy interest the information actually implicates. The SCA is filled with dichotomies and distinctions that form the basis of legal categories that are treated differently under the statute.[25] The statute draws distinctions between content and non-content information, voluntary and compelled disclosure, public and nonpublic service providers, and communication and computing

[20] Kerr, *supra* note 18, at 1210.

[21] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that there is no expectation of privacy for dialed phone numbers conveyed to telephone companies); United States v. Miller, 425 U.S. 435, 443 (1976) (holding that there is no expectation of privacy for deposit slips and checks given to a bank). The Court in *Miller* emphasized:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [them] to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Miller, 425 U.S. at 443. However, this doctrine is evolving in the modern age. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (refusing to extend the third-party doctrine to cell-site location information that is automatically sent to wireless carriers); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that there is a reasonable expectation of privacy in the *contents* of an email held on third-party servers).

[22] *See* S. REP. NO. 99-541, at 3 (1986). More recent jurisprudence has drawn a distinction between non-content online information, which is not protected by the Fourth Amendment, and content information, which may be. *See* Kerr, *supra* note 18, at 1210–11 nn.12–14.

[23] *See* S. REP. NO. 99-541, at 3, 5; H.R. REP. NO. 99-647, at 19 (1986).

[24] *See* S. REP. NO. 99-541, at 5.

[25] *See* Kerr, *supra* note 18, at 1223–34.

services.[26] Based on these distinctions, the statute provides differing levels of privacy protection. For example, greater privacy protection is afforded to content information, providers of services to the public, and communication services than to their respective counterparts.[27] The tiered protection mechanism of the SCA reflects the drafters' judgments about what kinds of information concern greater privacy interests and thus deserve greater protection.

Combining the legislative history of the SCA and its structured protection mechanism reveals a concrete aim. The purpose of the SCA is to cover the gaps in Fourth Amendment privacy protections for online communications, but only to provide just enough protection as is necessary, depending on the seriousness of the privacy interests involved.

2. *The Structure of the Stored Communications Act*

At its core, the SCA serves its purpose by limiting certain types of service providers from either voluntarily disclosing their subscribers' communications or being compelled to do so, while also balancing the interests of law enforcement.[28] To illustrate, service providers included under the SCA can knowingly divulge their users' communications *only* to the addressee or intended recipient of such communication, with the consent of the originator or the addressee of the communication, to a governmental entity "if the provider . . . believes that an emergency involving danger of death or serious physical injury . . . requires disclosure,"[29] or under a few other circumstances listed in 18 U.S.C. § 2702(b). Similarly, covered service providers cannot be forced by the government to divulge their users' communications except via a warrant, subpoena, or court order (depending on the type of service provided).[30] As such, communications held by covered service providers are afforded significant privacy protections.

The SCA, however, does not apply to all online and electronic services; it only provides privacy protections for communications held by two types of service providers: providers of electronic communication services (ECS) and providers of remote computing services (RCS).[31] This is because in 1986 these were essentially the only two types of online services offered: communication services, for sending and receiving messages such as email, and remote

[26] *See* 18 U.S.C. §§ 2702–03.

[27] *See id.*; *see also* Kerr, *supra* note 18, at 1222–33 (discussing in much greater detail the SCA's structured protection mechanism and dichotomies).

[28] *See* 18 U.S.C. §§ 2702–03.

[29] 18 U.S.C. § 2702(b)(8).

[30] 18 U.S.C. § 2703.

[31] *See* 18 U.S.C. §§ 2702–03.

computing services, for storage and outsourcing computing tasks.[32] It is clear that communication services implicate privacy concerns. Users have an interest in keeping their private messages private, even though such services typically make copies and store those messages while in flight. Oftentimes, communication services store private messages in temporary electronic storage for several months for user benefit and system integrity.[33] Likewise, remote computing services implicate similar privacy concerns.[34] Users send their private information to storage or outsourcing services, which then keep copies of that information for extended periods of time.[35]

By only regulating ECS and RCS providers, the SCA thus "freez[es] into the law the understandings of computer network use as of 1986."[36] Because the SCA provides different levels of regulations for ECS and RCS providers,[37] it is implicit that a service cannot be, at one time, both an ECS and an RCS. Therefore, current SCA jurisprudence requires delineating services as either ECS, RCS, or neither. Courts, however, often find it difficult to adjudicate modern cases under the statute, as services do not neatly fall into one category or the other.[38] Nonetheless, figuring out the exact classification of a service is particularly important, as that determines not only if, but also under what standards, the provider is regulated and its communications protected by the SCA.

a) Electronic Communications Services

An electronic communications service is "any service which provides . . . the ability to send or receive wire or electronic communications."[39] Under the SCA, a public ECS provider is prohibited from voluntarily sharing the contents of its stored user communications to any third parties, save for specified exceptions listed in § 2702(b).[40] Importantly, "contents" has an expansive meaning within the SCA. It encompasses not just

[32] *See* S. REP. NO. 99-541, at 3 (1986).

[33] *See id.*

[34] *See id.*

[35] *See id.*

[36] Kerr, *supra* note 18, at 1214.

[37] *See* 18 U.S.C. §§ 2702–03.

[38] *See, e.g.*, Flagg v. City of Detroit, 252 F.R.D. 346, 360–63 (E.D. Mich. 2008) (discussing whether SkyTel provided ECS or RCS in relation to stored text messages and admitting that its conclusion might be "mistaken").

[39] 18 U.S.C. § 2510(15).

[40] 18 U.S.C § 2702(a)(1).

the actual substance of a communication, but also "any information concerning the . . . purport, or meaning of that communication."[41]

The SCA further regulates how a governmental entity may *require* the disclosure of communications or records stored by ECS providers. The statute requires a warrant to compel disclosure of communication contents stored for 180 days or less.[42] There are less stringent requirements, such as requirements for only a subpoena or a court order, for communications held longer than 180 days[43] and for non-content information, such as user records.[44]

b) Remote Computing Services

On the other hand, a remote computing service is one that offers computer storage or processing services.[45] Unlike the near-absolute prohibition on voluntary disclosure of ECS-held communications, the analogous prohibition on RCS-held communications is much weaker. The SCA prohibits RCS providers from voluntarily sharing their stored user content only if three qualifying conditions are all met: (1) the content is carried strictly on behalf of a customer; (2) the content is carried solely for providing storage or processing services; and (3) the provider is not authorized to access the content for any reason other than providing storage or processing services.[46]

The SCA also regulates compelled disclosures of information held by RCS providers. The disclosure protections here are also much weaker than those available to ECS providers. To even be eligible for compelled disclosure protections, an RCS provider has to meet the same three qualifying conditions outlined in the preceding paragraph.[47] Even if the conditions are met, a governmental entity can require disclosure from an RCS provider much more easily than from an ECS provider. To compel disclosure of user content, the government can either (1) obtain a warrant or (2) provide notice to the subscriber and obtain a subpoena or court order.[48] For non-content information, the government needs only a subpoena or a court order; it does not need to notify the subscriber.[49]

[41] 18 U.S.C § 2510(8).
[42] 18 U.S.C § 2703(a).
[43] 18 U.S.C § 2703(b).
[44] 18 U.S.C § 2703(c).
[45] 18 U.S.C § 2711(2).
[46] 18 U.S.C § 2702(a)(2).
[47] 18 U.S.C § 2703(b)(2).
[48] 18 U.S.C § 2703(b).
[49] 18 U.S.C § 2703(c).

c) Significance of the Classification; Difficulty in Classifying

As the discussion, *supra*, illustrates, a service's classification as an ECS or an RCS is significant because it has a tremendous impact on the scope of privacy protections afforded to user information. Not only does the SCA provide generally weaker protections to information held by RCS providers, but it also conditions those protections on the RCS providers meeting the three qualifying conditions. One of the practical effects of these conditions, and one that is central to this paper, is that if an RCS provider is permitted to access its user communications for any reason unrelated to storage or processing, its stored information receives no disclosure protections. On the other hand, there is no such restriction for ECS providers.

While it is extremely important to delineate services as an ECS, RCS, or neither, it is often difficult and tricky to do so, as many modern service providers are multifunctional and provide multiple different services.[50] A specific entity, providing just a single service, "can act as [a] provider[] of ECS in some contexts, [a] provider[] of RCS in other contexts, and as neither in some contexts as well."[51] Further, many modern entities provide a plethora of different services (e.g., Google provides email, chat, maps, search engine, storage, document editing, and many other services). As such, courts have observed that defining whether an entity provides ECS or RCS is a context-specific inquiry. The distinction between the two "serves to define the service that is being provided at a particular time (or as to a particular piece of

[50] Courts also find the classification difficult due to an "inherent structural flaw[] in the statute." *See* Eric R. Hinz, Note, *A Distinctionless Distinction: Why the RCS/ECS Distinction in the Stored Communications Act Does Not Work*, 88 NOTRE DAME L. REV. 489, 501 (2012). There is uncertainty over whether storage "for purposes of backup protection" should be read expansively or narrowly. *Id.* If a communication is stored for backup purposes, then the service is an ECS; otherwise, the service is an RCS (or neither).

[51] Kerr, *supra* note 18, at 1215. Professor Kerr further explains that an entity can act as an ECS provider, RCS provider, or neither with respect to not only different communications, but also with respect to different copies of the same communication.

> In the case of a public provider, for example, files held in intermediate "electronic storage" are protected under the ECS rules; meanwhile, files held for long-term storage by that same provider are protected by the RCS rules. The same treatment exists for different copies of the same communication: a provider can act as an ECS with respect to one copy of a communication, as an RCS with respect to another copy, and as neither an ECS nor an RCS with respect to a third copy.

Id. at 1216 (footnotes omitted).

electronic communication at a particular time), rather than to define the service provider itself."[52]

d) Calls to Modernize the SCA

As the SCA was adopted in 1986 and was "written prior to the advent of the Internet and the World Wide Web,"[53] courts have often called upon Congress to modernize the SCA. In *Konop v. Hawaiian Airlines*, the Ninth Circuit stated that "the [SCA] is ill-suited to address modern forms of communication," and that "[c]ourts have struggled to analyze problems involving modern technology within the confines of this statutory framework."[54] The *Konop* court noted that "until Congress brings the laws in line with modern technology, protection of the Internet and websites . . . will remain a confusing and uncertain area of the law."[55] Similarly, in 2013, a frustrated federal district court wrote that "[m]ost courts, including this one, would prefer that Congress update the [SCA] to take into account the invention of the Internet."[56] While discussing the shortcomings of the SCA, courts have also specifically pointed out the difficulties in determining the scope of the statute's application to social media platforms and communications.[57]

III. *FACEBOOK V. SUPERIOR COURT OF SAN DIEGO COUNTY*

With the background of the SCA in mind, Part III of this Note turns to *Facebook v. Superior Court*, where the business model theory most recently materialized. Section III.A summarizes the case and the majority opinion as background, since the case was decided on separate grounds not involving the applicability of the SCA to social media companies. Section III.B of this Part then analyzes Chief Justice Cantil-Sakauye's concurrence, in which she explored the business model theory in greater depth.

[52] *In re* United States, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009).

[53] *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

[54] *Id.*

[55] *Id.*

[56] Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 666 n.2 (D.N.J. 2013).

[57] State v. Johnson, 538 S.W.3d 32, 68 (Tenn. Crim. App. 2017); *see also In re* Application of State for Commc'ns Data Warrants to Obtain the Contents of Stored Commc'ns from Twitter, Inc., 154 A.3d 169, 177 (N.J. Super. Ct. App. Div. 2017) ("Courts have expressed frustration with the failure to update the federal statute to keep pace with the advent of the Internet and social media platforms . . . .").

A. SUMMARY OF THE CASE AND MAJORITY OPINION

In *Facebook*, a defendant on trial for attempted murder by shooting sought to subpoena his victim's Facebook communications.[58] The defendant, Lance Touchstone, argued that he needed his victim's Facebook communications, both before and after the shooting, to investigate an affirmative self-defense claim and to impeach the victim's character.[59]

Facebook moved to quash the subpoena, but the superior court denied the motion, finding that there was good cause.[60] After a timely appeal by Facebook, however, the Supreme Court of California remanded the case to the superior court with directions to vacate its order. The California Supreme Court held that the trial court "erred by conducting an incomplete assessment of the relevant factors and interests."[61] The court used this case to point out the relevant seven factors ("Alhambra factors") that a court "should explicitly consider and balance in ruling on a motion to quash a subpoena . . . directed to a third party."[62]

By deciding and remanding the case based on the foundational issue of subpoena validity, the court did not have a chance to address the defendant's business model theory. The defendant argued that due to Facebook's business model, Facebook could not use the SCA as a shield to protect itself from non-compliance with the defendant's subpoena.[63] Since Facebook mines, analyzes, and shares information about its users' communications to facilitate targeted advertisements, the defendant asserted that the SCA's disclosure protections, codified in 18 U.S.C. §§ 2702(a) and 2703(b), did not apply and that Facebook must therefore comply with the subpoena.[64] And while Facebook urged the court to address this substantive issue, the court, noting the issue's importance, declined to do so, as it had disposed of the case on other grounds.[65]

[58] Facebook, Inc. v. Superior Ct. of San Diego Cnty., 471 P.3d 383, 387 (Cal. 2020).

[59] *Id.*

[60] *Id.* at 399.

[61] *Id.* at 387.

[62] *Id.* The seven factors were originally articulated in *City of Alhambra v. Superior Court*, 252 Cal. Rptr. 789 (Ct. App. 1988), *superseded in part by constitutional amendment*, CAL. CONST. art. I, § 30(c), *as recognized in Garcia v. Superior Court*, 163 P.3d 939, 946–48 (Cal. 2007), and consist of: (1) a "plausible justification," (2) the adequacy of description of the materials sought, (3) the availability of the sought materials from other sources, (4) whether any rights of the third party or "any protected governmental interest" would be violated, (5) the timeliness of the request, (6) the potential of delay of trial, and (7) whether there would be an undue burden on a document-producing third party. *Id.* at 799–800.

[63] *Facebook*, 471 P.3d at 402.

[64] *Id.* at 402–03.

[65] *Id.* at 402.

B. CHIEF JUSTICE CANTIL-SAKAUYE'S CONCURRENCE

Realizing the importance and potential implications of the defendant's business model theory, Chief Justice Cantil-Sakauye wrote a separate concurrence to explore the theory in more detail.[66] The Chief Justice first gave an overview of the business model argument, then provided background by reviewing the SCA's definition of ECS and RCS, and then lastly summarized the parties' contentions regarding Facebook's ECS/RCS status.

At a high level, the Chief Justice characterized the business model theory as an attack that sought to place Facebook and other similarly situated social media services "outside the ambit of . . . the Stored Communications Act."[67] The theory asserts that a service's "authorization to undertake, and its practice of" accessing its users' communications outside of certain limited circumstances "renders [the service] subject to a viable state subpoena."[68] For example, a service that mines, analyzes, and shares its subscribers' communications, or is authorized to do so, is precluded "from qualifying under the SCA *as a provider that is prohibited by the Act from disclosing user content*."[69] Therefore, such a service "cannot hold up the Act as a shield that protects it from complying with a viable state subpoena."[70]

In particular, the Chief Justice interpreted the business model theory as arguing that a service that accesses its users' communications for reasons outside the listed circumstances in the SCA "does not qualify as an entity that provides either ECS or RCS with respect to the sought communications."[71] The SCA only "covers, and prohibits disclosure of" communications held by ECS and RCS providers.[72] If an entity does not provide either in regard to a specific communication, "the entity cannot rely upon the SCA" to protect itself against a valid subpoena seeking that particular communication.[73]

When defining ECS and RCS, the Chief Justice emphasized the limitations put upon qualifying service providers in the disclosure provisions of §§ 2702(a) and 2703(b). As described above, an ECS provider is barred from knowingly divulging the contents of any stored user communications.[74] For RCS, the Chief Justice noted that several legal commentators, relying on the statutory

[66] *Id.* at 403–04 (Cantil-Sakauye, C.J., concurring).

[67] *Id.* at 403.

[68] *Id.* at 404.

[69] *Id.* at 404–05.

[70] *Id.* at 405.

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *See* 18 U.S.C. § 2702(a)(1).

language of § 2702, have reasoned that if an entity is "'authorized to access the contents of any [RCS communications] for purposes . . . other than storage or computer processing' . . . the Act's bar on disclosure is inapplicable. In other words, . . . such an entity would not be acting as an RCS."[75]

With the business model theory described and the ECS/RCS definitions reviewed, the Chief Justice considered the parties' arguments as to whether Facebook provided ECS, RCS, or neither. The criminal defendant argued that Facebook does not act as an ECS provider, as "(1) Facebook is authorized to [and does] mine, analyze, and share with third party advertisers licensed information about its users' content . . . , and (2) Facebook stores users' communications indefinitely, lets users share the stored data with others, and facilitates manipulation of the data by the user."[76] Facebook, on the other hand, asserted that it qualified as an ECS provider, as it either kept its users' communications in "temporary or intermediate storage" or stored them "for purposes of backup protection."[77] It further insisted that having access to its users' content was irrelevant in determining whether it was an ECS provider, and stated that a number of courts had already found it to be an ECS provider.[78]

In analyzing these arguments, the Chief Justice first noted that determining the ECS/RCS status of a service is a "context-dependent inquiry" that defines the service in relation to a particular communication at a particular time.[79] The Chief Justice pointed to federal decisions that held that when services such as email hold a message after it has been opened or accessed, the service transforms from an ECS to an RCS.[80] The Chief Justice analogized those cases to the current one. She thus stated,

> [W]hether Facebook should be found to qualify as a provider of ECS . . . appears open to question. Moreover, assuming that Facebook might qualify initially . . . as an entity that provides ECS, it . . . may also be obligated to establish its qualification as an entity that provides RCS with respect to stored communications sought in a viable state subpoena.[81]

[75] *Facebook*, 471 P.3d at 406 (Cantil-Sakauye, C.J., concurring) (quoting 18 U.S.C. § 2702(a)(2)(B)) (footnote and emphasis omitted).

[76] *Id.* at 408.

[77] *Id.* (quoting 18 U.S.C § 2510(17)).

[78] *Id.*

[79] *Id.*

[80] *Id.* at 409.

[81] *Id.*

The Chief Justice then analyzed the parties' arguments about whether Facebook qualified as an RCS provider. The Chief Justice first reiterated that due to the statutory language of § 2702, several legal commentators and at least one court had found that if an entity is authorized to access its users' communications for purposes other than providing storage or computer processing, "the entity may not, or does not, qualify under the SCA as one that provides RCS."[82] Using this argument, the criminal defendant asserted that since Facebook, as necessitated by its business model, does mine, analyze, and share information about its users' content with their authorization, it cannot qualify as an RCS provider.[83] Following this argument, those activities went beyond merely providing storage or processing services and "demonstrate[] that Facebook is authorized to act *in precisely the manner the statute says it must not* if it wishes to qualify as a provider of RCS."[84] Facebook, on the other hand, contended that everything it was authorized to do fell under the umbrella of computer processing services.[85] The Chief Justice noted that Facebook cited a federal decision, legislative history, and an academic article by Orin Kerr to support its claim, all allegedly showing that computer processing services should be broadly construed.[86] Unconvinced, the Chief Justice questioned whether those sources really supported Facebook's assertion; in fact, she stated that the sources "may suggest the opposite—that ['computer processing services'] was intended to have a narrow, rather than broad, interpretation."[87]

Facebook also argued that every court that had previously considered whether Facebook was qualified as an ECS or RCS provider found that it met at least one of the tests.[88] The Chief Justice, however, remained unconvinced and simply stated that no court had ever considered the criminal defendant's specific claim that due to Facebook's business model, it did not qualify as an ECS or RCS provider, thus falling outside the purview of the SCA.[89] That issue remains unresolved.[90]

Going beyond the statutory language and precedent, Facebook also asserted that its policy considerations necessitated that it qualified under the SCA. "[C]oncluding otherwise would (1) unduly disrupt and impair technological innovation, (2) disappoint users' settled privacy expectations,

[82] *Id.*

[83] *Id.* at 409–10.

[84] *Id.* at 410.

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] *Id.*

and (3) frustrate its ability to protect against malware."[91] Citing "practical marketplace reasons," the Chief Justice questioned whether disqualifying Facebook as a protected entity under the SCA would actually lead to "disruptions or voluntary disclosures . . . absent legal compulsion."[92] Further, the Chief Justice stated that a narrower construction of "computer processing" could still include measures to counteract malware, while excluding mining and analyzing user data for targeted advertisements.[93] Finally, the Chief Justice stated that "as a matter of policy, . . . finding Facebook to lie outside the SCA might have the beneficial effect of spurring long-needed congressional adjustment of the outdated [Stored Communications] Act."[94]

IV. PROPOSED FRAMEWORK AND APPLICATIONS

With an understanding of the SCA in place and with the basic structure and mechanisms of the business model theory explained by Chief Justice Cantil-Sakauye, this Note can now turn to its analysis. In this Part, this Note first analyzes how the business model theory affects modern social media services and their disclosure protections under the SCA. Section IV.A gives a brief critique of the Chief Justice's concurrence in *Facebook* to highlight key interpretative differences in the business model theory. This Note then discusses its three-step analytical framework in Section IV.B, with the hopes of giving courts a systematic way of analyzing modern services under the SCA. Following the introduction of this framework, Section IV.C demonstrates its application to three web services. Finally, Section IV.C uses the worked-out examples to draw out general lessons and extrapolations to reach an overall conclusion: the business model theory will not have a noticeable effect on social media services and their disclosure protections.

A. CRITIQUE OF THE CHIEF JUSTICE'S CONCURRENCE

The Chief Justice's brief analysis of the business model theory, though helpful in outlining the theory's main ideas and arguments, had a few notable shortcomings. First, and most importantly, the Chief Justice overgeneralized the business model theory. She interpreted it to mean that a successful business model attack rendered a service completely outside the purview of the SCA, instead of just the SCA's disclosure provisions. Second, the Chief Justice failed to acknowledge the underlying strangeness of the business model theory:

[91] *Id.*

[92] *Id.* at 410–11.

[93] *Id.* at 411 n.14.

[94] *Id.*

mainly that the theory further punishes consumers for a service's insecure or privacy-harming business model (e.g., a service that shares user data with third parties for ad targeting). Finally, while the Chief Justice made a valid point that marketplace concerns will prevent services from carelessly sharing user data even without the SCA protections in place, such important privacy rights deserve to be statutorily protected anyway.

Throughout the concurrence, the Chief Justice overgeneralized the business model theory. Relying on the criminal defendant's characterization and a number of legal scholars, the Chief Justice interpreted the theory as stating that an electronic communication or computing service, by accessing or having the authority to access user communications for reasons other than providing communication, storage, or processing functions, could not be classified as an ECS or RCS, thus falling completely outside of the SCA's scope.[95] The business model theory, when more properly stated, is more focused; it is better interpreted as asserting two specific claims. First, if an ECS's business model requires it to share user communications to third parties, it violates § 2702(a)(1), which bars an ECS provider from "knowingly divulg[ing]"[96] user communications. Second, and much more significantly, the business model theory states that if an RCS has the authorization to access user communications outside of providing storage or processing services, that RCS falls outside of the disclosure provisions set forth in §§ 2702(a)(2) and 2703(b), making its communications unprotected from voluntary and compelled disclosures. Importantly, the business model theory does not remove the service from being an ECS or RCS; the service still retains its classifications and is still bound by the rest of the SCA.[97] It is simply the disclosure provisions that are violated or no longer apply.

The Chief Justice's overgeneralization of the business model theory was largely dependent on conflating the conditions of the disclosure provisions with the actual definitional requirements of ECS and RCS. The definition of ECS, set out in § 2510(15), states that an ECS is "any service which provides . . . the ability to send or receive wire or electronic communications."[98] If an ECS shares its stored communications to third parties, as it is prohibited to do under disclosure provision § 2702(a)(1), it

[95] *See id.* at 405–06, 408–10.

[96] 18 U.S.C. § 2702(a)(1).

[97] For example, an RCS that accesses its user communications for reasons unnecessary to provide storage or processing services loses SCA §§ 2702(a) and 2703(b) disclosure protections for its user communications. However, it is still bound by § 2703(c), which governs compelled disclosures of subscriber records and information.

[98] 18 U.S.C. § 2510(15).

merely violates that subsection;[99] it still remains an ECS. Similarly, the definition of RCS is set out in § 2711(2) and means any service that provides the public "computer storage or processing services."[100] If an RCS is authorized to access its users' communications for reasons unrelated to computer storage or computer processing, it simply means that the RCS fails the condition to receive disclosure protections under §§ 2702(a)(2) and 2703(b). The service still remains an RCS, but its stored communications are no longer protected.

Further, the Chief Justice failed to address the inherent oddity in the business model attack, which further punishes consumers for a service's already problematic business model. Boiled down, the RCS prong of the SCA ends up stripping people of their online privacy because an RCS provider is using a business model that itself decreases user privacy (i.e., requiring authorization to access user communications for non-storage or non-processing reasons). In effect, a successful business model attack harms user privacy because user privacy is already being harmed.

Proponents of the business model theory may argue that when users authorize a service provider to access their communications for reasons unrelated to the central (i.e., storage or processing) service, the users no longer have an expectation of privacy. And while this argument may have made sense in the 1980s, where online services only had one function and were not so intrinsically linked with our day-to-day lives, it no longer holds weight. Most modern entities are multifaceted and provide several different services, both ECS and RCS. When a user authorizes an entity to access their information, they do so by agreeing to a privacy or a data policy that concerns the entity as a whole. Most policies do not differentiate between services, and as such do not differentiate the authorizations given to ECS components versus RCS components. Therefore, courts should not be looking at authorization in the abstract, as that deals with the entire entity. Instead, courts should be looking at if and how the RCS components actually access user information.

From a more policy-oriented perspective, online services are now so linked with our daily lives that it is wrong to say that because a user authorizes a company to access their data to accomplish non-storage/non-processing

[99] 18 U.S.C § 2707(a) provides that "[any] subscriber, or other person aggrieved by any violation of this chapter . . . may, in a civil action, recover from the person or entity . . . which engaged in that violation such relief as may be appropriate." 18 U.S.C. § 2707(a). Section 2707(b) lists three appropriate remedies available to plaintiffs who bring a civil action under the SCA: "preliminary and other equitable or declaratory relief," damages, and reasonable attorney's fees and costs. 18 U.S.C. §§ 2707(b)(1)–(3).

[100] 18 U.S.C. § 2711(2).

tasks, they no longer deserve any privacy protection. And while marketplace concerns[101] make it unlikely that online entities would voluntarily disclose user communications, such privacy rights are so important that they deserve to be statutorily protected regardless. Relying on an entity's goodwill and reputational concerns is not good enough.

B. PROPOSED ANALYTICAL FRAMEWORK

While Chief Justice Cantil-Sakauye's concurrence in *Facebook* provides insight into the business model theory, how it might apply to Facebook, and the potential policy considerations it implicates, the theory still "deserves additional and focused attention."[102] Given social media's pervasive nature and ever-growing influence in our society, it is vital to understand how the business model theory affects the SCA disclosure protections provided to social media communications.[103]

A closer look at the business model theory reveals that it has a minimal impact on disclosure protections provided to most social media services. Due to the inherent communicative purpose of social media and the nature of modern ad-targeting business models, where user data is neither shared nor sold, the business model attack largely falls flat. Nevertheless, due to the numerous services and business models available, business model scrutiny, which is too-often ignored and disregarded by current courts, is an important step in SCA analysis. Courts should make a conscious effort to add this step into their analysis to better and more fully determine the scope of a service's disclosure protections. In particular, courts should implement business model scrutiny as one step within a three-step analytical framework when analyzing modern services under the SCA.

The three-step framework is meant to serve as a structuring tool, leading courts to a more concrete and systematic analysis of services under the SCA. In the first step, courts should classify the service in question as an ECS, RCS, or neither. This is likely the most arduous step in the framework. In the second step, assuming that the service fits as an ECS or RCS, courts should identify the service's business model and determine exactly what authorizations the service has to access consumer data. In the third and final step, courts should determine how the service's business model and authorizations to access and use user data impact the service's compliance with the SCA's disclosure provisions. Specifically, if the service is an ECS and divulges user

[101] Facebook, Inc. v. Superior Ct. of San Diego Cnty., 471 P.3d 383, 410–11 (Cal. 2020) (Cantil-Sakauye, C.J., concurring).

[102] *Id.* at 411.

[103] *Id.* at 412 (Cuéllar, J., concurring).

communications to third parties, it violates the SCA and can be liable for civil damages.[104] If the service is an RCS and has authorization to or does access consumer data for reasons other than providing storage or processing services, its user communications are not protected from disclosures under the SCA.

This analytical framework is necessary given that there is little statutory guidance in applying the SCA to modern technologies and services, leaving courts confused and frustrated.[105] Left to their own devices, courts currently engage in a case-by-case, ad-hoc analysis, which often leaves important steps ignored, such as business model scrutiny. This also results in hard-to-understand opinions and weak analysis, which further muddies the water.

1. Step One: Classification of Service as an ECS, RCS, or Neither

Here, courts should use traditional analytical methods, shaped by statutory interpretation, precedent, peer courts, and academic and legal research, to determine the classification of a service as an ECS, RCS, or neither. Courts should keep in mind that this is a context and fact-specific inquiry that defines not the entire entity or corporation, but rather the specific service as it relates to a particular piece of information at a particular time.[106]

a) Determining Whether a Service is an ECS

As defined *supra*, an ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[107]

In order to add certainty and avoid contravention of the statute's intent, courts should classify a service as an ECS if the relevant piece of communication can be viewed and edited or responded to by at least one non-sending, non-service party. This conception would modernize the SCA by adding certainty as to whether certain modern services can be classified as an ECS or not. For example, it would definitively allow providers of emails, chats, wall and forum posts, tweets, shared pictures, and editable documents to be considered ECS providers. Recipients of these communications can message back, leave a comment, "like" the photo, or edit the shared documents.

[104] *See supra* note 99.

[105] *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002); Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 666 n.2 (D.N.J. 2013); State v. Johnson, 538 S.W.3d 32, 68 (Tenn. Crim. App. 2017); Anzaldua v. Ne. Ambulance & Fire Prot. Dist., 793 F.3d 822, 839 n.5 (8th Cir. 2015).

[106] *See In re* United States, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009); Flagg v. City of Detroit, 252 F.R.D. 346, 362 (E.D. Mich. 2008); *Facebook*, 471 P.3d at 408 (Cantil-Sakauye, C.J., concurring); Kerr, *supra* note 18, at 1215 & n.48.

[107] 18 U.S.C. § 2510(15).

Therefore, a service in relation to such a communication can be quickly and easily classified as an ECS, at least for certain periods of time.

The requirement that at least one other party can view or respond to the communication also ensures that the service is actually being used to communicate and share information, rather than being used for rudimentary storage or backup purposes. Thus, if a person sends a message or email to only themself or changes their privacy settings so that their tweets or wallposts are only visible to themself, the service, in that particular situation, is not acting as an ECS. This would prevent anyone from "gaming" the SCA by making it seem like they are sending communications, when in reality they are just storing information (as ECS communications are provided higher privacy protections than RCS communications). A change in privacy settings of a particular communication, therefore, may lead to a change in classification of that service. For example, if a user posts a picture on Facebook for their friends, but then changes the privacy settings so that only they can still see the picture, Facebook would go from an ECS provider to an RCS provider or neither in that context.

As services can change between ECS, RCS, and neither even in relation to a specific piece of communication, timing plays an important role in the service's classification. For instance, multiple courts have held that webmail services are ECS while an email is in transit and sits unopened by the recipient, but transform into RCS once that email has been accessed.[108] As Professor Orin Kerr notes,

> The thinking is that when an e-mail customer leaves a copy of an already accessed e-mail stored on a server, that copy is no longer "incident to transmission" nor a backup copy of a file that is incident to transmission: rather, it is just in remote storage like any other file held by an RCS.[109]

[108] *See, e.g.*, United States v. Weaver, 636 F. Supp. 2d 769, 772–73 (C.D. Ill. 2009); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635–38 (E.D. Pa. 2001), *vacated in part on other grounds*, 352 F.3d 107 (3d Cir. 2003). *But see* Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2004) (holding that an email on a server, regardless of whether it has been accessed, is protected under the ECS rules until "the underlying message has expired in the normal course"); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902–03 (9th Cir. 2008) (re-affirming *Theofel's* holding that an ECS that stores an already-accessed communication remains an ECS indefinitely), *rev'd on other grounds sub nom.* City of Ontario v. Quon, 560 U.S. 746 (2010). The view espoused by *Theofel* has been attacked by courts and legal scholars. *See Weaver*, 636 F. Supp. 2d at 772–73; Kerr, *supra* note 18, at 1217 & n.61.

[109] Kerr, *supra* note 18, at 1216. This thinking also comports with legislative intent. *See* H.R. REP. NO. 99-647, at 64–65 (1986) (noting that an accessed email still kept on a provider's server is covered under sections relating to remote computing services).

This reasoning can be easily extended to text and online chat messages; if the message has been accessed by the intended recipient but is still stored by the service, the service is acting as an RCS in regard to the recipient's copy of the communication.[110]

If courts cannot easily tell when the communication has been opened or accessed, they should default to the 180-day lifespan for ECS communications asserted in the SCA; thereafter, they should treat the service as an RCS. For communications such as tweets or wallposts, where there is just one copy of the communication that is viewable by a large group of "friends" or "followers," determining when every "friend" has accessed the communication would be tough, if not impossible. Courts can thus grant those communications perpetual protection under the ECS provisions, but this is likely to be unsatisfactory; not only would this treat tweets and wallposts differently from email and chat, but it would also seem illogical to say that an entity is still providing an electronic communication service in relation to a message posted, say, five years ago. Instead, courts should use the SCA-drawn lifespan for ECS communications, 180 days, as the default upper limit. Section 2703(a) provides strong protection against required disclosures for ECS contents held in electronic storage for 180 days or less.[111] It provides weaker protection for contents held in storage for longer than 180 days; the protection given to contents in long-term storage is the same as that afforded to contents held by RCS providers.[112] Courts should use this distinction and hold that once a provider stores an ECS communication for longer than 180 days, the service transforms to an RCS in relation to that communication.[113]

This Part's conception of ECS keeps pace with modern developments while still pursuing the statutory purposes of the SCA and remaining faithful to legislative intent and court precedent. The 1986 House Report on the SCA classified "electronic bulletin boards," which offer "interested persons [the ability to] communicate openly with the public to exchange . . . information," as a feature, specifically, of some *electronic communication services*.[114] As such, courts have repeatedly held that bulletin board services are protected under

[110] *See Flagg*, 252 F.R.D. at 362–63 (holding that Skytel, a text message service provider, was initially an ECS provider, but transformed into an RCS provider after the communication in question was accessed and stored).

[111] *See* 18 U.S.C. § 2703(a).

[112] *See id.*

[113] *See* Kerr, *supra* note 18, at 1217 n.61.

[114] H.R. REP. NO. 99-647, at 62 (1986).

the SCA,[115] and at least two courts have explicitly found that such services fall under the umbrella of ECS.[116] The electronic bulletin boards of 1986 can be easily analogized to present-day forums, such as Reddit, and to services that offer wallposts, tweets, and multimedia sharing, such as Facebook, Twitter, and Instagram.[117] Like bulletin boards, these modern day services allow users to share thoughts and information: a user can post a particular topic, which may come in the form of a thread, a wallpost, or even a picture, and other users can respond with their thoughts, opinions, or additional information. Protecting these services under ECS, which is afforded stronger protections than RCS, would further the purpose of the SCA; it would provide strong Fourth Amendment-like protections to online social communications that implicate important privacy interests.

b) Determining Whether a Service is RCS

If a service is not classified as an ECS, courts then have to determine if the service is an RCS. As defined in § 2711(2), a remote computing service is "the provision to the public of computer storage or processing services."[118]

As a threshold matter, courts should only question whether a service is an RCS if they have already concluded that it is not an ECS. This is because communications held by ECS providers are afforded greater privacy protections than those held by RCS providers.[119] Thus, if a particular service can be classified as both an ECS and an RCS in regard to a particular communication, it should by default be considered an ECS and the communication afforded the appropriate protections. To do otherwise would be to provide lesser, RCS-style protections to a communication technically held by an ECS; this would go against the terms of the SCA. Relatedly, by only reaching the RCS determination inquiry after holding that the service failed to

[115] *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002).

[116] *See Konop*, 302 F.3d at 875, 879; Kaufman v. Nest Seekers, LLC, No. 05 CV 6782 (GBD), 2006 WL 2807177, at *5 (S.D.N.Y. Sept. 26, 2006). *But see* Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 443 (W.D. Tex. 1993) (finding that a bulletin board service was an RCS), *aff'd*, 36 F.3d at 457.

[117] *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980–81 (C.D. Cal. 2010) (finding Facebook and Myspace wallposts to be analogous to bulletin board services).

[118] 18 U.S.C. § 2711(2).

[119] *See* 18 U.S.C. § 2702(a) (providing a blanket prohibition against voluntary disclosure of ECS-held communications but requiring multiple conditions for the prohibition to apply to RCS-held communications); 18 U.S.C. § 2703 (generally requiring a warrant to compel disclosure of ECS-held communications, but only a subpoena or court order for an RCS-held communication).

qualify as an ECS, courts can preempt the question asking whether all modern, online ECS providers, because they invariably require storage and processing functionalities, necessarily provide RCS as well. While courts can dispose of this question by (1) noting that the SCA specifically protects ECS communications "in electronic storage"[120] and then differentiating electronic storage from the RCS conception of storage and by (2) highlighting the higher level of protections afforded to ECS communications, this question merely serves to distract and confuse courts. This question is simply unnecessary, as once an ECS determination has been made, the classification inquiry should stop.

In regard to RCS, the concept of computer storage is relatively straightforward. It simply refers to storing information on another entity's servers for either space, backup, or user convenience considerations. There are countless services in the market that specialize in offering such services: some of the more popular ones today are Dropbox, Google Drive, and Microsoft OneDrive. Additionally, computer storage service also incorporates services that were ECS but transformed into RCS. As described above, if a communication service retains the communication after the recipient has already accessed it, or if the service stores the communication for longer than 180 days, the service transforms from an ECS into an RCS.[121] It makes sense to conceptualize those "drop-down" services as providing computer storage.

Defining processing services, however, is more difficult. In an abstract sense, every modern online technology can be described as a processing service. When you interact with an online service, the service processes your inputs and provides you with the appropriate output(s). For example, when you use a search engine, the search engine processes each keystroke, displaying them on your monitor. Once the query is typed up and you hit the "Search" button, the search engine searches its index for the appropriate content, ranks it in terms of relevancy (usually), and then displays the results.[122] Similarly, when you are online shopping and click on a link for "Men's Shoes," the service pulls up its list of men's shoes for sale, ranks them using some algorithm (e.g., popularity over the last quarter), and then displays the results. If you then sort by "Price Low–High," the service changes the order of the results to show you the cheapest shoes first.

[120] *See* 18 U.S.C. § 2702(a)(1).

[121] *See supra* Section IV.B.1.a.

[122] Britney Muller, *How Search Engines Work: Crawling, Indexing, and Ranking*, MOZ, https://moz.com/beginners-guide-to-seo/how-search-engines-operate [https://perma.cc/U9KK-3AC3] (last visited Aug. 17, 2022).

Legislative history, however, shows that the drafters of the SCA meant processing services to be more narrowly defined. The Senate Report talks about "businesses of all sizes transmit[ting] their records to remote computers to obtain sophisticated data processing services."[123] This shows that the legislators intended "processing services" to mean those used when outsourcing tasks and functions. "In the era before spreadsheets, a company might send raw data to a remote computing service and ask the service to crunch numbers to calculate its payroll."[124] As such, processing services, in relation to the SCA, should only include services that are used when outsourcing "sophisticated" data processing or other computationally-intensive tasks. Currently, some popular processing services include Amazon AWS, Microsoft Azure, and Google Cloud. These services may be used to run analytics on Big Data, train Artificial Intelligence, provide network security and monitoring, render animations, and much more.

2. *Step Two: Analyzing the Service's Business Model and Interaction with Consumer Data*

If courts have classified a service as an ECS or RCS, as opposed to neither, they should then determine the data authorizations the service has and how and why it interacts with consumer data. Here courts should specifically look for whether the service divulges its users' communications to third parties or if it has authorization to and does access its users' communications for reasons unnecessary to the service it provides. Such disclosures or data accesses would implicate violations of the SCA or disqualify the service from the SCA's disclosure provisions (as examined in Step Three).[125]

Scrutinizing a service's business model may entail examining the company's annual reports, reading the company's data, privacy, and security policies, analyzing the dominant models used by the company's peers, and simply asking or requiring the company to disclose its pertinent model(s). It is important to note, however, that the business model of interest is that of the service, and not of the entire entity. A few high-level examples of business/revenue models include selling consumer data, using targeted advertisements, and selling additional or premium features for a cost.

Courts should then seek to understand if, how, and why the service accesses user data in relation to its business model. This will likely require reading and understanding the service's data and privacy policies. It should be noted, however, that it might be difficult to disentangle how and why different

[123] *See* S. REP. NO. 99-541, at 3 (1986).

[124] Kerr, *supra* note 18, at 1230.

[125] *See* 18 U.S.C. §§ 2702(a), 2703(b).

services of a particular company access consumer data; most policies are written to apply one set of rules to an entity's entire suite of services, rather than different sets to different services. More precisely, courts should look at the service's treatment of the particular content or communication in question, as that will ultimately decide if the service is violating the SCA or is disqualified from the SCA's disclosure provisions in regard to that distinct communication.

If the service is an RCS, courts should ask if users have specifically authorized the service, and not the entire entity, to access their data for any reasons unrelated to providing storage or processing services. This is an extremely difficult question because, as noted above, privacy and data policies are not usually separated service-by-service or by ECS vs. RCS components. A user authorizing an entity to access its data is not the same as the user authorizing the specific RCS component. Therefore, courts should also look to whether the RCS actually accesses user data for non-storage or processing reasons, as that is likely the best proof of authorization. If appropriate, courts can also ask if users can change the service's authorization settings. If so, courts should then look at the actual authorization settings in play, as they relate to particular communications at the time of the inquiry.

If the service is an ECS, courts should ask if the service knowingly shares or sells its users' communications to third parties. These ECS and RCS specific questions are important, as they will guide the courts in Step Three when determining whether the service violates or is disqualified from the disclosure provisions of the SCA.

3. *Step Three: Determining Whether the Service's Business Model Violates the SCA or Disqualifies It from the SCA's Disclosure Provisions*

Once courts understand the service's business model and how and why it interacts with consumer data, they should look at §§ 2702 and 2703 and determine if the service violates or is disqualified from the SCA's disclosure provisions. Section 2702(a)(1) states that an ECS provider cannot "knowingly divulge" or share its users' communications to third parties.[126] On the other hand, RCS-held user communications are only protected from voluntary or compelled disclosure if the provider is not authorized to access its users' communications for any reason other than providing computer storage or processing services.[127]

As such, if the service is classified as an ECS, and the service does knowingly divulge the contents of the user communications in question, then

[126] *See* 18 U.S.C. § 2702(a)(1).

[127] *See* 18 U.S.C. §§ 2702(a)(2), 2703(b).

the service violates the voluntary disclosure provision set out in § 2702(a)(1) and would be liable for civil penalties.

Similarly, if the service is classified as an RCS, and is authorized to access the communication in question for any non-storage or non-processing reasons, then the service is disqualified from the voluntary and compelled disclosure provisions set forth in §§ 2702(a)(2) and 2703(b). In other words, the RCS provider can share user information with who and whatever it wants, and it must comply with simple government subpoenas. However, as explained in Step Two, it is very difficult to see if a particular RCS service or functionality actually has that authorization. Therefore, courts, in most circumstances, should look to actual access and not just authorization (which tends to be entity-level authorization) when determining whether the RCS provider should be disqualified from the SCA disclosure provisions. That is, courts should only disqualify an RCS provider if it actually accesses user communications for reasons unrelated to computer storage or processing.

Further, courts should interpret the disqualifying condition narrowly, allowing RCS providers to access consumer data not just for the core storage or processing service, but also for all supplementary services necessary to maintain system integrity, preserve user security, and provide a viable and robust service. Such a conception would afford service providers flexibility in ensuring that their service remains secure, complies with present or future regulations regarding content monitoring, and provides useful functionalities such as email search. This way, if a storage service accesses the consumer data to scan for malware[128] or provide search results, the consumer data can still qualify for disclosure protections.

C. EXAMPLES OF USING THE ANALYTICAL FRAMEWORK

With the proposed analytical framework explained, it would be beneficial to see how it works on modern online services. First, Part C first analyzes Gmail's webmail service through the lens of the three-step framework. This example shows how the framework works in a scenario already analyzed by and litigated in courts (i.e., scrutinizing email/webmail under the SCA), thus serving as a tool to make baseline comparisons and expectations. Further, this example also illustrates the intricacies of the SCA and demonstrate how services are moving towards (or already using) an ad-based business model that does not analyze user communications. Second, Part C analyzes Facebook's

[128] *See* Davey Winder, *Google Confirms New AI Tool Scans 300 Billion Gmail Attachments Every Week*, FORBES (Feb. 28, 2020, 7:35 AM), https://www.forbes.com/sites/daveywinder/2020/02/28/google-confirms-new-ai-tool-scans-300-billion-gmail-attachments-every-week/?sh=812e4b3edd1f [https://perma.cc/S5CV-SQUX].

Messenger service. This example shows how most, if not all, messaging services can be directly analogized to email for analysis under the SCA. Third, Part C applies the three-step framework to Facebook Wallposts. This example covers non-messaging social media services where the communications are often sent to mass groups of people ("friends" or "followers") while having no "read receipt" feature, showing how the lack of the feature creates unique challenges under the current SCA jurisprudence that the proposed framework and conceptualizations help mitigate.

1. *Gmail*

Imagine Person A, who uses Gmail, sending an email to Person B who, for simplicity's sake, also uses Gmail. As Person A writes the email, a "draft" is created and periodically saved. Once A finishes writing and sends the email to Person B, the draft is completed and Gmail removes the "Draft" label and affixes the "Sent" label to the email. This way, if A wants to read the email again, they can do so by clicking on the "Sent" label and accessing all the sent emails.[129] At the same time, a copy is created and sent to Person B's inbox, where it is affixed with the "Inbox" label. Therefore, there are (at least) two copies: Person A's copy with the "Sent" label and Person B's copy with the "Inbox" label.

a) Step One: Determining if Gmail is an ECS, RCS, or Neither

Determining whether Gmail is an ECS, RCS, or neither depends on which copy of the email is in question. For example, if the government is trying to compel disclosure of Person *A*'s copy (either while in the "draft" stage or after it was sent), then Gmail is acting as an RCS, not an ECS. In either the draft or the sent stage, Person *A*'s copy cannot be viewed, edited, or responded to by any other non-sending, non-service party. It also cannot be said that either copy is in "intermediate storage . . . incidental to the electronic transmission" of the communication or that either copy is being stored for "backup protection" in relation to a communication service.[130] It is more compelling to think of Gmail indefinitely storing Person *A*'s copy as providing a storage service for user convenience, i.e., later access by Person *A*.

In regard to Person *B*'s copy of the email, Gmail's status as an ECS or RCS depends on whether Person *B* has accessed the email or not. As described above,[131] if Person *B* has not yet accessed the email, then the email remains in

[129] *See* Facebook, Inc. v. Superior Ct. of San Diego Cnty., 471 P.3d 383, 372 n.14 (Cal. 2020) (Cantil-Sakauye, C.J., concurring).

[130] *See* 18 U.S.C. §§ 2510(17)(A)–(B).

[131] *See supra* Section IV.B.1.a.

"intermediate storage . . . incidental to the electronic transmission," and Gmail still serves as an ECS.[132] On the other hand, if Person *B* has already accessed the email, then Gmail, in relation to that particular email, is an RCS: the email "is no longer 'incident to transmission[,]' . . . it is just in remote storage like any other file held by an RCS."[133]

In sum, Step One finds that Gmail is an RCS with respect to Person *A*'s copy, and that Gmail is an ECS *or* RCS with respect to Person *B*'s copy, depending on timing.

b) Step Two: Gmail's Business Model and Interactions with Data

Gmail has two primary business models. There is a paid version of Gmail sold to businesses as part of Google Workspace, a collection of productivity and "collaboration tools like Gmail, Calendar, Meet, Chat, Drive, Docs, . . . and more."[134] There is also a free version of Gmail that serves "useful and relevant," i.e., targeted, ads to its users.[135] This Section will focus on the free version of Gmail and how it interacts with its subscribers' communications.

While Gmail's free version uses targeted ads, it does not share user content with third parties. Gmail's targeted ads are "shown to [a person] based on [their] online activity while [they're] signed into Google."[136] Google does not "scan or read . . . Gmail messages to show . . . ads."[137] Further, Google "does not sell . . . personal information," nor does it "share . . . personal information with advertisers, unless [a subscriber] ha[s] asked [them] to."[138] Gmail also allows users "[t]o opt-out of the use of personal information for personalized

[132] *See* 18 U.S.C. § 2510(17)(A).

[133] Kerr, *supra* note 18, at 1216.

[134] GOOGLE WORKSPACE, https://workspace.google.com/ [https://perma.cc/3TKF-JTH9] (last visited Aug. 17, 2022).

[135] *How Gmail Ads Work*, GMAIL HELP, https://support.google.com/mail/answer/6603?hl=en&ref_topic=3394218 [https://perma.cc/85QP-XNHF] (last visited Aug. 17, 2022).

[136] *Id.*

[137] *Id.* It is worthwhile to note that Google did scan user emails for ad personalization in the past. It stopped this practice in mid-2017. Daisuke Wakabayashi, *Google Will No Longer Scan Gmail for Ad Targeting*, N.Y. TIMES (June 23, 2017), https://www.nytimes.com/2017/06/23/technology/gmail-ads.html [https://perma.cc/NS28-U5YZ]. Even so, the analysis would still remain the same for pre-2017 emails—courts should look at the actual authorization settings in play at the time of the inquiry when determining the scope of the SCA protections. Doing otherwise would, at least to a certain extent, render user authorization changes moot. This can upset user privacy expectations and can lead to fractured protections, depending on how often the authorization settings are changed.

[138] *How Gmail Ads Work*, *supra* note 135.

Gmail ads" by "turn[ing] off Ads Personalization."[139] From this information it is evident that, at the very least, Gmail does not access or share user content for targeted advertisements.

While Gmail does not access emails for ad targeting, it does access them to provide user convenience functionalities. For example, Gmail has a search functionality that allows a user to find particular emails by typing in key words or filling in who the sender or recipient was. To present relevant results, Gmail must scan the user's emails to determine which ones appropriately match the inquiry. Further, Gmail also has a function that automatically tags some emails as important. "Gmail analyzes [a user's] new incoming messages to predict what's important, considering things like how [they've] treated similar messages in the past, how directly the message is addressed to [the user], and many other factors."[140] Users can opt out of this functionality. There are many other Gmail functionalities, such as auto-categorization of social media emails, spam and malware detection, and reply and follow-up reminders, that involve Gmail accessing user communications.

In sum, Step Two finds that while Gmail accesses user communications, it does so for supplementary services needed to provide user and system integrity and user convenience.

c) Step Three: Determining Whether Gmail Violates or is Disqualified from the Disclosure Provisions of the SCA

First, turn to Person A. Under the SCA, in order for RCS communications to qualify for disclosure protection, the RCS must not have authorization to access user communications for reasons other than providing storage or processing services.[141] As found in Step Two, while Gmail may not access its user emails to provide targeted advertisements, it still does so to provide several supplemental functionalities, such as search, spam detection, and auto-categorization. For some of these services, such as search and follow-up reminders, Gmail accesses user emails while serving as an RCS. Such functionalities, however, should be looked at as necessary for providing a modern, robust email service. Realistically, no email service can survive without a built-in search function. These functionalities exist to enhance user convenience by providing a service where a user can easily access and interact

[139] *Id.*

[140] Anne P. Mitchell, *Gmail 'Skip the Inbox' Filter Not Working? This May Be Why – and How to Fix It*, INTERNET PATROL (Apr. 8, 2019), https://www.theinternetpatrol.com/gmail-skip-the-inbox-filter-not-working-this-may-be-why-and-how-to-fix-it [https://perma.cc/NZ22-WBME].

[141] *See* 18 U.S.C. §§ 2702(a)(2), 2703(b).

with their past emails. As such, these supplementary services should be conceptualized under the umbrella of storage services. And as § 2702(a)(2) extends protection as long as the RCS is only authorized to access user content for storage or computing services, Person A's copy of the email should be protected from voluntary and compelled disclosure.

Now turn to Person B. As seen in Step One, Gmail may either be acting as an ECS or an RCS, depending on whether B has accessed the email or not. If Person B has not accessed the email, then Gmail is acting as an ECS. And as established in Step Two, Gmail does not share the contents of email communications to third parties for advertising purposes. As such, it is unlikely that Gmail shares user communications for any other reason as well. Under this assumption, Gmail, acting as an ECS, does not violate the SCA's voluntary disclosure provision set forth in § 2702(a)(1). If Person B has accessed the email, then Gmail is acting as an RCS. Here, the same reasoning would apply as it did for Person A's email—Gmail, as an RCS, would not be disqualified from the SCA's disclosure provisions, and Person B's email would be protected.

2. *Facebook Messenger*

Now instead of an email exchange, imagine Person A and Person B talking over Facebook Messenger. As in the Gmail example, begin by examining Person A sending a message to Person B. When Person A sends the message, a copy is retained on Person A's chat window, and another copy is sent to Person B's. The analysis in Step One, determining whether Messenger is an ECS, RCS, or neither, is the same as in the Gmail example; messaging and text services can be easily analogized to email services. Messenger, in relation to Person A's copy of the message, acts as an RCS. In relation to Person B's copy, Messenger acts as an ECS if *B* has not yet accessed the message, and an RCS otherwise.

Similar to Gmail, Messenger does not "use the content of . . . messages . . . for ad targeting,"[142] and it does not sell information to advertisers.[143] Instead, targeted ads are shown "based on [the user's] activity across Meta technologies," the user's "activity with other businesses," the user's "activity on other websites and apps," and the user's location.[144]

[142] *You Control Your Messenger Experience*, MESSENGER, https://www.messenger.com/privacy [https://perma.cc/6KGL-85ES] (last visited Sep. 8, 2022).

[143] *About Facebook Ads*, FACEBOOK, https://www.facebook.com/ads/about/?entry_product=ad_preferences [https://perma.cc/P6A6-U4AX] (last visited Aug. 17, 2022).

[144] *Id.*

Messenger, however, does scan and collect information from chats to "improve the product experience[] and keep people safe and secure."[145] For example, Messenger automatically scans chat messages to stop scammers, prevent phishing, safeguard minors,[146] protect users from malware and viruses, and prevent the spread of child exploitation imagery.[147] Further, users can report a chat as violating Facebook's "[C]ommunity [S]tandards," which may prompt human moderators to take a look at the chat and take it down.[148]

While some of these services, such as search or account investigations, involve Messenger accessing user communications as an RCS for reasons unrelated to storage, they still do not disqualify Messenger from the RCS disclosure provisions of the SCA. As in the Gmail example, these functionalities should be seen as supplementary to providing a robust and user-friendly storage service that protects its users and maintains both system and entity integrity. As such, Messenger, as an RCS, should not be disqualified from the SCA's disclosure protections.

Similarly, Messenger, acting as an ECS, does not violate the SCA disclosure provision set forth in § 2702(a)(1). It does not share or knowingly divulge its user communications with third parties, and thus complies with the provision.

3. *Facebook Wallposts*

Here, imagine Person A posting a status onto their "Facebook Wall." Unlike the Gmail and Messenger examples, there is only one copy of the message—Person A's. By default, only A's Facebook friends can view the wallpost, and they can do so either by going to Person A's profile or by exploring their own "Newsfeed." The analysis done here can be analogized to picture and video sharing services, forums, and other status-update/profile-creation services, such as Twitter and LinkedIn.

a) Step One: Determining if Facebook is an ECS, RCS, or Neither

Facebook, in relation to Person A's wallpost, should be regarded as an ECS for the first six months. The post is viewable by A's friends, who can comment on it, "like" it, or share it, giving credence to the notion that Facebook is acting as a communication service.

[145] *You Control Your Messenger Experience*, *supra* note 142.

[146] *Id.*

[147] Alanna Petroff, *Yes, Facebook is Scanning your Messages for Abuse*, CNN BUS. (Apr. 5, 2018, 10:18 PM), https://money.cnn.com/2018/04/05/technology/facebook-messenger-messages-privacy/index.html [https://perma.cc/Y95K-4JM7].

[148] *See id.*

The wallpost can be further analogized to a post made on a private electronic bulletin board service. As described above, courts have repeatedly held that electronic bulletin boards come under the purview of the SCA.[149] And while courts are more split on whether bulletin board services are ECS or RCS, legislative history seems to favor the ECS conception.[150] Using this bulletin board analogy, the court in *Crispin v. Christian Audigier, Inc.* held that Facebook, in relation to a wallpost, is an ECS.[151] In so concluding, the court reasoned that wallposts must be "stored for backup purposes," as they could not be "protectable as a form of temporary, intermediate storage."[152] For Facebook wallposts, "there is no temporary, intermediate step . . . . Unlike an email, there is no step whereby a Facebook wall posting must be opened, at which point it is deemed received."[153] The better conception, however, is that the wallpost is in temporary storage. While Facebook is the literal "final destination"[154] of the wallpost, in a more real sense the final destinations are the actual recipients. This is the same reason why even though a recipient's inbox is the final destination of an email, the email is still considered to be in temporary storage until it is accessed. Therefore, Person A's wallpost should be considered an electronic communication held in temporary storage.

As it is understandably difficult, or even impossible, to confirm when all of A's friends have accessed the wallpost, Facebook should remain an ECS for the default, SCA-drawn lifespan of 180 days.[155] After that time, Facebook should be thought of as an RCS in relation to *A*'s wallpost. At that point, the wallpost should be considered to be in remote storage.

b) Step Two: Facebook's Business Model and Interactions with Consumer Data

Facebook, like most social media companies, relies on a business model built on targeted ads. Although it relies on ad targeting, Facebook does not "sell any [user] information to anyone, and . . . never will."[156] It does, however, share limited information with partners and advertisers. The information

[149] *See supra* note 115 and accompanying text.

[150] *See supra* note 114 and accompanying text; Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002).

[151] *See* 717 F. Supp. 2d 965, 988–89 (C.D. Cal. 2010).

[152] *Id.* at 989.

[153] *Id.*

[154] *Id.* at 988 (quoting Snow v. DIRECTV, Inc., No. 2:04-CV-515FTM33SPC, 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005), *report and recommendation adopted*, 2005 WL 1266435 (M.D. Fla. May 27, 2005), *aff'd*, 450 F.3d 1314 (11th Cir. 2006)).

[155] *See supra* note 113 and accompanying text.

[156] *Data Policy*, FACEBOOK (Aug. 21, 2020), https://www.facebook.com/full_data_use_policy [https://perma.cc/8UJ7-G4XJ].

shared is "aggregated statistics" and "reports about the kinds of people" that interact with the advertiser's Facebook Pages, posts, and advertisements; importantly, Facebook does not share user communications with third parties.[157]

Nonetheless, in order to personalize ads and provide an integrated experience across its numerous products, Facebook has the authorization to, and does, collect "the content [and] communications" that users provide when using their products.[158] Facebook uses this information to provide, personalize and improve their products."[159] In essence, this means that they "connect information" across Facebook Products in order to provide a seamless experience and to better tailor ads.[160] At a broad level, in selecting what ads to show a particular individual, Facebook uses location data; profile information, such as age, gender, education, job title, and relationship status; interests, including listed hobbies, activities, and page interactions; and behaviors, such as mobile and device usage.[161]

Like Messenger, Facebook, aside from collecting user information for ad personalization, also scans and collects information to provide supplementary services necessary to "[p]romote safety, integrity and security."[162] Facebook uses this information to "combat harmful conduct, detect and prevent spam and other bad experiences, . . . [and] investigate suspicious activity or violations of [Facebook's] terms or policies."[163]

c) Step Three: Determining Whether Facebook Violates or is Disqualified from the Disclosure Provisions of the SCA

In the first six months, while Facebook is acting as an ECS in relation to A's wallpost, Facebook will not violate the disclosure provision set forth in § 2702(a)(1) of the SCA. As Facebook does not sell or share the contents of a user's wallposts (or any other user communications, for that matter), it does not "knowingly divulge . . . the contents of a communication" to a third party.[164] Therefore, it complies with the ECS disclosure provision of the SCA.

[157] *See id.*

[158] *Id.*

[159] *Id.*

[160] *See id.*

[161] *See id.*; *About Reaching New Audiences*, FACEBOOK FOR BUS. (Nov. 11, 2020), https://www.facebook.com/business/help/717368264947302?id=176276233019487&helpref=page_content [https://perma.cc/4TYS-84WH].

[162] *See Data Policy*, *supra* note 156.

[163] *Id.*

[164] *See* 18 U.S.C. § 2702(a)(1).

Perhaps counterintuitively due to its ad personalization, Facebook, acting as an RCS in relation to *A*'s wallpost after 180 days, will not be disqualified from the voluntary and compelled disclosure provisions of the SCA. Facebook is authorized to and does access user communications, including wallposts, for several reasons, including search, suspicious activity investigation, and spam and malware detection. Many of these interactions, however, happen while Facebook is acting as an ECS, i.e., shortly after the communication is posted.[165] For example, Facebook has a number of A.I. systems that can automatically detect, and sometimes take down, hate speech, misinformation, pornography, and other policy-violating materials.[166] After Facebook has transformed into an RCS, however, its communication interactions are likely limited to search and user report investigations. Like with Messenger, these interactions should be viewed as supplementary to providing a secure and user-friendly storage service.

Specifically in regard to targeted advertisements, Facebook does not mine or analyze wallposts to personalize ads. Rather than analyzing status updates and posted pictures, Facebook looks at profile information, life updates, listed hobbies, and user interactions with business and interest pages. Even if wallposts were analyzed for ad purposes, it is likely that the analysis would happen shortly after the communication was posted and then be quickly integrated into the user's ad profile. It is unlikely that Facebook would analyze a wallpost 180 days or later for ad personalization. As such, Facebook, acting as an RCS in respect to *A*'s wallpost, should not be disqualified from the voluntary and compelled disclosure provisions of the SCA.

D. LESSONS AND EXTRAPOLATIONS FROM USING THE FRAMEWORK

In each of the Gmail, Messenger, and Facebook examples above, the business model theory did not hold that the service was either violating or disqualified from the disclosure provisions of the SCA. For most social media services, this result is to be expected as a consequence of the information-sharing nature of these services and the ad-targeting business models they apply.

[165] *See generally* Jeremy Kahn, *Facebook Makes Strides Using A.I. to Automatically Find Hate Speech and COVID-19 Misinformation*, FORTUNE (May 12, 2020, 11:21 AM), https://fortune.com/2020/05/12/facebook-a-i-hate-speech-covid-19-misinformation [https://perma.cc/T7U9-EX72] (explaining that Facebook's A.I. systems are getting better at automatically detecting and removing hate speech and misinformation).

[166] *See id.*; Mark Sullivan, *Facebook's AI for Detecting Hate Speech is Facing its Biggest Challenge Yet*, FAST CO. (Aug. 14, 2020), https://www.fastcompany.com/90539275/facebooks-ai-for-detecting-hate-speech-is-facing-its-biggest-challenge-yet [https://perma.cc/65CP-6KQ3].

As social media has a general communicative purpose, with users sharing information with their friends and followers, it is compelling to think of these services as ECS. Subscribers use these services to connect with others, participate in conversations, and share various parts of their lives. As such, courts will likely see many of these services as providing, in relation to most pieces of information, "the ability to send or receive . . . electronic communications."[167] Of course, as described above in the Gmail and Facebook examples, some of these services will "drop down" to RCS when the communication in question has been accessed or when enough time, i.e., 180 days, has passed.

Further, even though the business model of most social media services is based on targeted advertisements, that fact is unlikely to prevent the services from complying with the SCA. Most popular social media services do not actually sell or share user communications with third parties to facilitate their ad targeting; indeed, data policies often explicitly state that the service does not sell or share user content.[168] As such, when these services are acting as ECS in relation to a particular communication, they will not be found to violate the disclosure provisions of the SCA.

It is also unlikely that social media services, when they "drop down" to RCS, will be disqualified from receiving voluntary and compelled disclosure protections under the SCA. Most major social media services do not scan and analyze user communications for ad personalization; instead, the services rely on, amongst other things, demographics, profile information, and specified interests.[169] And even if these services were to scan communications for ad

[167] *See* 18 U.S.C. § 2510(15).

[168] *See, e.g.*, *Data Policy*, *supra* note 156 ("[Facebook does not] sell any of your information to anyone, and [they] never will."); *Twitter Privacy Policy*, TWITTER (June 18, 2020), https://twitter.com/en/privacy [https://perma.cc/WL35-NWT6] ("[Twitter] use[s] information about whom you have communicated with and when (but not the content of those communications) . . . ."); *Reddit Privacy Policy*, REDDIT (Sept. 15, 2020), https://www.redditinc.com/policies/privacy-policy-october-15-2020 [https://perma.cc/PY9H-TKSZ] ("Reddit only shares nonpublic information about you in the following ways. We do not sell this information."); *Privacy Policy*, SNAP INC. (Sept. 14, 2020), https://www.snap.com/en-US/privacy/privacy-policy [https://perma.cc/59EW-QUA4].

[169] *See* Petroff, *supra* note 147; *How Gmail Ads Work*, *supra* note 135. The fact that social media services do not analyze user communications is most apparent through privacy/data policies and instructional web pages sharing how the service actually personalizes ads. *See, e.g.*, *About Reaching New Audiences*, *supra* note 161; *Targeting Options for LinkedIn Advertisements*, LINKEDIN HELP, https://www.linkedin.com/help/lms/answer/722/targeting-options-for-linkedin-advertisements?lang=en [https://perma.cc/R4JM-W3HR] (last visited Aug. 17, 2022); *About Targeting for Video Campaigns*, YOUTUBE HELP, https://support.google.com/youtube/answer/2454017?hl=en [https://perma.cc/UVJ2-34TG] (last visited Aug. 17, 2022).

personalization, it is likely to happen early after a communication is posted, while the service is still acting as an ECS.[170] Further, while many social media services have authorization to access user communications for functionalities such as search and user report investigations, these functionalities should be considered supplementary to the core RCS, and thus allowed.

While the business model theory will not diminish the disclosure protections afforded to most social media services, courts should still use business model scrutiny and the three-step framework in their analysis. Due to the sheer and expanding number of social media services and the various business models available, it is still important to use context-specific, case-by-case analysis. Courts should consider each service separately and, using business model scrutiny and the three-step framework, should determine if the social media service violates or is disqualified from the disclosure protections of the SCA. Adhering to this framework will result in better reasoned and structured analysis, which will not only be responsive to modern technologies and services, but will also help clarify the muddy waters of SCA jurisprudence.

V. CONCLUSION

The proposed framework and conceptualizations laid out in this Note would help modernize courts' understanding of the SCA and guide them through this murky and confusing area of the law. The framework helps courts supplement their analysis, strengthen their structure, and provide consistent results. Moreover, the modernized conceptualization of the SCA underlying the framework helps resolve the main inherent oddity of the business model attack: it seeks to use a privacy statute to diminish the privacy rights of internet users, specifically in a context where they are already vulnerable. By viewing supplementary functionalities of services as a broader part of the service itself, courts can ensure that users and their communications are appropriately protected in the digital realm. When analyzing the business model attack through this modernized lens, a conclusion becomes clear: due to the nature of current ad-targeted business models, the attack will have little, if any, impact on social media services and their SCA disclosure protections.

[170] *See* 18 U.S.C. §§ 2702(a)(1)–(2). An RCS provider, if it wants to receive SCA disclosure protections, cannot access user communications for any reasons unrelated to providing storage and processing services. There is no such restriction for ECS providers. Therefore, an ECS service can access user communications for ad targeting.