TOURO LAW
JACOB D. FUCHSBERG LAW CENTER

Touro Law Review

Volume 37 | Number 3 Article 11

2021

Fixing What's Broken: The Outdated Guidelines of the SCA and Its Application to Modern Information Platforms

Lutfi Barakat
Touro Law Center

FIXING WHAT'S BROKEN: THE OUTDATED GUIDELINES OF THE SCA AND ITS APPLICATION TO MODERN INFORMATION PLATFORMS

Lutfi Barakat[*]

ABSTRACT

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) to afford privacy protections to electronic communications and it has not changed since its inception. The ECPA has proven problematic as technology has advanced, but Congress has not modified the law to reflect this change. Courts have struggled to apply the law to both old technologies that have been updated and new technologies that have emerged. The ECPA needs to be revised to reflect the new advances in technology or be repealed and replaced with a new approach. This will ensure that consumer data will be safeguarded while in the hands of data provider companies.

[*] J.D. Candidate 2021, Jacob D. Fuchsberg Touro Law Center. My interest in the subject of data protection stems from how extensive technology was a part of my upbringing. The amount of information and entertainment at my disposal not only kept me informed and distracted, but also made me want to ask questions. Is this website safe? Should I be uploading my sensitive information to this website? What is keeping my information safe? The rise of technology also brought with it the rise of hacking, something all of us have had to deal with at some point. The underlying goal of this note was to understand how the law has attempted to manage the internet and protect its users from the exploitation of others. The ultimate objective of this note is to propose changes to the current legal structure of data protection statutes to ensure stronger safeguards for our data and technologies.

I. INTRODUCTION

In the current technology-dependent age, the lack of safeguards against unreasonable invasions of consumer data from third parties poses troubling implications for consumers.[1] Back in 1986, Congress passed the Electronic Communications Privacy Act (ECPA) to afford privacy protections to electronic communications.[2] Title 1 of the ECPA amended the federal Wiretap Act to address the interception of electronic communications, while Title II created the Stored Communications Act (SCA) to handle access to stored wire and electronic communications and also transactional records.[3] Congress created the ECPA because it noted the "gap in protection and the potentially devastating effects it had on privacy."[4] However, times have changed and the technology available has changed also. Companies today maintain physical hard drives or servers of data with inadequate supervision, leaving them susceptible to breaches.[5] The companies escape blame by not actively taking part in divulging the information.[6] This information can come in the form of incoming and outgoing emails.[7] Companies can share such generally stored data with the government if it is for a legal purpose.[8] This applies even if the government entity obtained the information beyond the scope of its reach and the customer did not receive notice.[9] The Ninth Circuit Court of Appeals set a standard, known as the "knowingly divulged" standard first seen in *Theofel v. Farey-Jones*, that states if a defendant obtains consent through exploitation of a known mistake, such as going beyond the scope of a subpoena, he cannot seek refuge in that consent if it relates to the essential nature of his access.[10] The standard set by the Ninth Circuit, however, does

---

[1] Simon M. Baker, *Unfriending The Stored Communications Act: How The Technological Advancement And Legislation Inaction Have Rendered Its Protections Obsolete*, 22 DEPAUL J. ART TECH. & INTELL. PROP. L. 75, 78 (2011).
[2] Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002).
[3] *Id.*
[4] Baker *supra* note 1, at 80.
[5] *Id*.
[6] Theofel v. Farey-Jones, 359 F.3d 1066, 1072 (9th Cir. 2004).
[7] *Id*. at 1072.
[8] *Id.* at 1071.
[9] *Id.*
[10] *Id*. at 1073.

not take into account a company passively allowing the information of its customers to be undefended against intrusions resulting from mistakes such as overextending one's reach.[11] These passive breaches of consumer data protection occur because the SCA is outdated in light of today's modern technology that has far surpassed the current protections that were created in the 1980s.[12] The application of the SCA eventually made it into areas of private life, like social media, and produced confusing results.[13]

Despite the SCA's flaws, the Ninth Circuit will continue to use it until Congress acts. The Ninth Circuit has struggled to determine the law involving facets of social media such as "likes" and smartphones that gather geographic data, and has failed to address the inability for some providers to fit within the remote-computing services (RCS) and electronic communications services (ECS) categories of the SCA.[14] Companies that have allowed consumer data to be shared and taken by the government on the request of third parties should be held to a stricter standard as regulated in an amended version of the SCA or a completely new approach.

In *Theofel v. Farey-Jones*,[15] NetGate, an internet service provider ("ISP"), was forced to disclose emails on the order of a subpoena.[16] Farey-Jones' attorney was only supposed to request in the subpoena the relevant e-mails or e-mails from a certain period.[17] However, the subpoena was too broad in scope and time.[18] After discovering that the subpoena was invalid, rendering the disclosure of the emails improper,[19] the plaintiff brought a claim arguing that NetGate's consent to the subpoena was invalid.[20] The scope of the disclosure went to the heart of the subpoena, and as such, NetGate

---

[11] *Id.*
[12] Rudolph J. Burshnic, *Applying The Stored Communications Act To The Civil Discovery Of Social Networking Sites*, 69 WASH. & LEE L. REV. 1259, 1264 (2012).
[13] *Id.* at 1292-93.
[14] Cousineau v. Microsoft Corp. 6 F. Supp. 3d 1167 (W.D. Wash. 2014); Rainsy v. Facebook, Inc., 311 F. Supp. 3d 1101, 1106 (N.D. Cal. 2018); Quon v. Arch Wireless Operating Co., Inc. 529 F.3d 892 (9th Cir. 2008).
[15] *Theofel*, 359 F.3d at 1072.
[16] *Id.*
[17] *Id*. at 1071.
[18] *Id*. at 1072.
[19] *Id.*
[20] *Id.*

did not have the authority to relinquish control of its client's emails.[21] The Ninth Circuit coined the "knowingly divulged" standard, stating that if a mistake went to the essential nature of the invasion of privacy, it would invalidate such invasion.[22] This offense, however, is an exception, as the SCA, enacted in the 1980s, was not equipped to handle the problems caused by emails and social media, such as the scope and limitations of disclosing emails and the rise of social media and its features.[23] The ECS and RCS categories within the statute have not withstood the test of time, and new technologies such as social media are seemingly incompatible with it.[24] This Note will discuss the reasons the SCA should be amended, if not repealed as a whole.

Section II will explain the SCA's various provisions relating to the disclosure of data to third parties. Section III will examine both the Ninth Circuit's approach and the evolution of its standards during the past two decades. Section IV will focus, specifically, on the case of *Theofel v. Farey-Jones* and its articulation of the "knowingly divulged" standard. Section V will argue in favor of amending or repealing the SCA and discuss alternatives to better accommodate emerging technologies. Finally, Section VI will conclude that the SCA's flaws outweigh its usefulness, and it should be either amended or repealed.

II. THE ORIGINS OF THE SCA AND OTHER DATA PRIVACY LEGISLATION

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA)[25] to afford privacy protections to wired and stored communications.[26] Title I of the ECPA amended the federal Wiretap Act[27]which existed prior to the ECPA, and handled electronic communications, which consists of the information users share via websites.[28] The main objective of Title I is to protect the

[21] *Id.*
[22] *Id*. at 1073.
[23] Burshnic, *supra* note 12, at 1264.
[24] *Id*.
[25] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).
[26] *Id.*
[27] 18 U.S.C. § 2510
[28] *Id.*

privacy of persons in connection with the use of electronic and wire communications.[29]

Title II of the ECPA, also known as the SCA, is used by aggrieved parties seeking relief for breaches of their electronic information.[30] While the SCA was enacted in 1986 to address the lack of guidelines in the Fourth Amendment in the area of computer technologies, it failed to account for the internet and the possible ramifications the SCA could have on individual privacy.[31] The court in *Low v. LinkedIn Corp.*[32] explained that the SCA was enacted to assign criminal and civil liability "for certain unauthorized access to stored communications and records."[33] However, the SCA has a limited scope and does not address all online transgressions.[34] Specifically, the SCA prohibits entities that store information from "knowingly divulg[ing]" that information to other outside entities.[35] However, the Ninth Circuit has indicated that reckless and negligent conduct in maintaining user information only meets the "knowingly divulged standard" when the provider sends the information to a person or entity that is not the intended recipient.[36] This does not take into account the provider sending a certain amount of information that goes beyond the scope or limits of the disclosure. Despite the static nature of the SCA, Congress has not changed the statute and now the law is outdated and difficult to use.[37]

A. The SCA's Two Entities: RCS and ECS

The SCA focuses on two types of entities: RCS and ECS.[38] The SCA defines an RCS as a service that provides computer storage or processing services to the public through an electronic communications service.[39] In other words, RCS refers to an electronic communication service that stores and processes data of

[29] Freedman v. Am. Online, Inc., 325 F. Supp. 2d 638, 643 (E.D. Va. 2004).
[30] Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1022 (N.D. Cal. 2012).
[31] *Id.*
[32] 900 F. Supp. 2d 1010 (N.D. Cal. 2012).
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] Worix v. MedAssets, Inc., 857 F. Supp. 2d 699, 702 (E.D. Ill. 2012).
[37] Baker, *supra* note 1, at 78.
[38] *Id.* at 85
[39] *Id.* at 86.

consumers that subscribe to the service.[40] Next, the SCA defines an ECS as an entity that provides its users with the ability to send or receive wire or electronic communications.[41] For example, a provider that supplies email services would be considered an ECS.[42] An ECS, therefore, handles the actual transmission of that information, whether the information is being received or being transferred to another party.

Significantly, whether an entity is an RCS, ECS, or neither plays a critical role in asserting an entity's non-disclosure obligations.[43] If the entity is not in the RCS or ECS category, the entity can reveal or use the contents however it wishes.[44] Whether an entity is an ECS or RCS depends upon what information is disclosed.[45] It is common practice today for businesses to store their data with external providers.[46] Although most ISPs function as both, the distinction is important because different services offer different protections.[47]

B. SCA Punishment and Exceptions

The SCA specifies the punishment for violating the statute.[48] The statute provides punishment for offenses committed while attempting to gain "commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State."[49] If the offenders are found guilty under § 2701(b) of the SCA, they can receive a fine and up to ten years in prison, but if the offense cannot be categorized under § 2701(b), then the maximum sentence they can receive is a fine and five years.[50] Finally, the SCA provides exceptions to accessing content if the

[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.* at 87.
[46] *Id.*
[47] *Id.*
[48] 18 U.S.C.A. § 2701(b).
[49] *Id.*
[50] *Id.*

conduct was authorized.[51] Specifically, if access was authorized "by the person or entity providing a wire or electronic communications service," or, "by a user of that service with respect to a communication of or intended for that user," then no penalty would be applicable.[52]

In addition, Congress enacted the Computer Fraud and Abuse Act ("CFAA") in 1986 to address the problem of computer hacking.[53] It provides criminal penalties to those who accessed a computer without authorization to commit fraud.[54] The aggrieved party must show that the computer accessed was protected, the party attempting to gain access was not authorized to use the computer, that the party had the intent to commit the crime and the party defrauded the owner of something of value.[55]

III. CASES WHERE INADEQUATE SECURITY PRACTICES CAUSED INJURY

The courts in several cases determined that the companies that held the aggrieved parties' information had caused them injury through their inadequate security practices.[56] In *Low*, the court determined that the plaintiffs had brought an actionable cause for relief.[57] In that case, the plaintiffs suffered harm when LinkedIn transmitted their LinkedIn data, including their browsing history and identification to third parties as well as advertisers, marketing companies and data brokers.[58] This allowed third parties to recreate the plaintiffs' user identity and gather sensitive information about the plaintiff from their browsing history.[59] The court found that the plaintiffs' alleged violation of surveillance statutes gave it a

[51] *Id.* § 2701(c).
[52] *Id.*
[53] *Id.* at 1060.
[54] U.S. v. Nosal, 930 F. Supp. 2d 1051, 1057-58 (N.D. Cal. 2013).
[55] *Id*.
[56] *See* McDonald v. Kiloo ApS, 385 F. Supp. 3d 1022, 1033 (N.D. Cali. 2019); Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1022 (N.D. Cal. 2012); Freedman v. America Online, Inc., 325 F. Supp. 2d 638, 643 (E.D. Va. 2004); *In re* Pharmatrak, Inc., 329 F.3d 9, 20 (1st Cir. 2003); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001).
[57] *Low*, 900 F. Supp. 2d at 1022.
[58] *Id.* at 1017.
[59] *Id.*

"concrete" foundation that supported Article III standing.[60] The court disagreed that LinkedIn could be classified as an RCS or ECS because it did not meet the SCA standards.[61] The court found that LinkedIn was not an RCS because it was not holding or processing the offsite third party's information, specifically their profile URLs and their LinkedIn IDs.[62] This information was generated by LinkedIn itself and not sent by the users.[63] If LinkedIn could be categorized as an RCS or ECS it would have been held liable, but the court held that LinkedIn could not be categorized as an RCS.[64] LinkedIn does not take the user IDs and URLs and store them with a third party (in this case LinkedIn) and the same applies with the user.[65] Had LinkedIn functioned as an advanced computer program that processed information, it would have been classified as an RCS, but the court found otherwise.[66]

In *McDonald v. Kiloo ApS*[67] the district court decided that the plaintiffs had alleged an actionable claim for violation of the SCA against the companies holding and transmitting their data.[68] In that case, the plaintiffs sued both the developers of the apps their children used, Disney, Kiloo, and Viacom, as well as the SDK defendants.[69] The SDK defendants were a group of mobile advertising and monetization companies that provided kits for collecting user data.[70] The plaintiffs' complaints alleged that the SDK defendants were coordinating together to collect recovered data from children for the purpose of profiling and targeting children with specific advertisements.[71] To collect the data, Disney, Kiloo, and Viacom were provided a specific code that would transmit consumer data to the SDK for data tracking and ad targeting.[72] The extensive data gathered on the child-users allowed SDK to create sophisticated

[60] *Id.* at 1021.
[61] *Id.* at 1023.
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id*.
[66] *Id*.
[67] 385 F. Supp. 3d 1022, 1033 (N.D. Cal. 2019).
[68] *Id.*
[69] *Id.* at 1028.
[70] *Id.*
[71] *Id.* at 1029.
[72] *Id.*

profiles of the children.[73] SDK would then send their profiles to third parties, allowing third parties to target them with advertising based on those profiles.[74] Disney relied on New York General Business Law Section 349(a) to discredit the plaintiffs' claims.[75] To bring a violation of consumer protection under New York law, the plaintiffs had to show that the companies engaged in deceptive practices.[76] The court agreed that the breadth of the company's data collection efforts violated the New York statute and the plaintiffs were entitled to relief.[77]

The court held that the plaintiffs had introduced sufficient claims under the New York and California consumer protection statutes, stating respectively that the companies had indeed collected the information and utilized it under New York law, and that the collection of the data was unfair, unlawful, and fraudulent under California law.[78]

In *Freedman v. American Online, Inc.,*[79] the district court determined that the ISP, American Online (AOL), had a reasonable basis to question the validity of a warrant it received. In this case, an internet service subscriber sued two police officers and AOL for violating his rights when the officers accessed his private information retained by the provider in connection with an obscene email other parties had received.[80] The court stated that AOL met the "knowingly divulg[ing]" standard of the ECPA by transmitting the information to the Police Department after requesting it.[81] As a result, the court entered summary judgment for the plaintiff.[82] While AOL claimed that it did not have the requisite state of mind specified in the statute to knowingly divulge the information, since it relied on a defective warrant before divulging the consumer information to the police, the court rejected the defendant's contention.[83] The court stated that AOL did not need a specific state of mind; rather, it only

[73] *Id.*
[74] *Id.* at 1029.
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id*. at 1038-39.
[79] 412 F. Supp. 2d 174 (E.D. Va. 2004).
[80] *Id*. at 180.
[81] *Id.* at 183.
[82] *Id.* at 180.
[83] *Id.* at 183.

had to divulge the information to another party intentionally, regardless of the reason.[84]

The First Circuit Court of Appeals in *In re Pharmatrak, Inc.*[85] determined that defendant Pharmatrak's website intercepted the messages within the meaning of the ECPA.[86] The First Circuit agreed with the plaintiffs that the users of Pharmatrak's website, NETcompare, did not consent to the tracking of their information.[87] Pharmatrak used the information to analyze where on the website its users visited so Pharmatrak could compare the tracking information to Pharmatrak's competitors.[88] Although Pharmatrak stated to its clients that the cookies[89] it used to save data would not collect personal information, the personal information of over two hundred users was nonetheless found on Pharmatrak's servers.[90] The defense tried to argue that Pharmatrak did not meet the requirement of "intercepting" the communications as indicated in the statute.[91] The statute defined interception as the acquisition of any information through the use of an electronic device.[92] The website narrowed down the incoming communications to include interceptions that were contemporaneous with the transmission.[93] The court decided that it satisfied this stipulation; the GIF,[94] or the graphic interchange format, that enabled the interception to "sometimes arrive[d] before the content delivered by the pharmaceutical clients."[95] This interception happened either before or alongside the transmission.[96] The interception itself was done with NETcompare, an automatic routing program.[97] Automatic routing programs are the only exception to the principle that interceptions of emails that are not

[84] *Id.*
[85] 329 F.3d 9 (1st Cir. 2003)
[86] *Id*.
[87] *Id.* at 21.
[88] *Id.* at 13.
[89] *What is a cookie?*, ALL ABOUT COOKIES, https://www.allaboutcookies.org/cookies/ (last visited Apr. 3, 2021).
[90] *In Re Pharmatrak*, 329 F.3d at 14.
[91] *Id.* at 22.
[92] *Id.*
[93] *Id.*
[94] Andrew Heinzman, *What is a GIF, and how do you use them?* (Sept. 25, 2019) https://www.howtogeek.com/441185/what-is-a-gif-and-how-do-you-use-them/.
[95] *In Re Pharmatrak*, 329 F.3d at 22.
[96] *Id.*
[97] *Id*.

already prohibited by the Wiretap Act are impossible.[98] Therefore, the court decided that, despite its intentions, Pharmatrak had intercepted its clients' data and violated the ECPA.[99]

In *EF Cultural Travel BV v. Explorica, Inc.*[100] the First Circuit determined that the defendant, Explorica, had violated the CFAA in taking pricing data.[101] Explorica was formed by ex-members of EF ("Education First") Cultural Travel as well as other institutions, and decided to compete in the teenage touring industry.[102] The defendant used a scraper program that collected pricing information from EF and its users, allowing it to undercut EF's prices in the tour market.[103] Once this came to light during litigation regarding an individual's departure from EF, the United States District Court for the District of Massachusetts found that Explorica had exceeded authorized access into EF's servers.[104] The First Circuit affirmed, holding that EF exceeded the reasonable limits of its authorization when it began taking proprietary information.[105]

In *Suzlon Energy Ltd. v. Microsoft Corp.*,[106] the Ninth Circuit determined that the ECPA was meant to offer protection to any person, regardless of the status of his or her United States citizenship.[107] The defendant Suzlon sought emails in a server maintained by Microsoft to use in a civil fraud proceeding against an Indian citizen.[108] Microsoft argued that the disclosure of these emails would violate the ECPA, stating that the emails had to be discoverable in a foreign proceeding and that the subpoenas had to comply with the Federal Rules of Civil Procedure.[109] The Ninth Circuit found otherwise, saying that the ECPA provided disclosure to any person, without any qualification.[110] A plain reading of the statute indicates that it would naturally include foreign citizens as

---

[98] *Id.*
[99] *Id.*
[100] 274 F.3d 577, 579 (1st Cir. 2001).
[101] *Id.*
[102] *Id.* at 580.
[103] *Id.*
[104] *Id.*
[105] *Id.* at 583-84.
[106] 671 F.3d 726, 728 (9th Cir. 2011).
[107] *Id.*
[108] *Id.* at 727.
[109] *Id.*
[110] *Id.* at 729.

well.[111] The court also stated that this protection applies not only to acquisition by government entities, but also to civilian entities.[112] With this decision, the Ninth Circuit effectively extended the protections of the ECPA to foreign citizens and would next target social media corporations.

A. SCA's Impact on Social Media

Despite the challenges and uncertainties of applying the SCA and ECPA to innovations such as social media, the court utilized them in its decision in *Crispin v. Christian Audigier Inc.* [113] in a case involving Facebook.[114] Before *Crispin*, the District Court for the Central District of California in *Quon v. Arch Wireless Operating Co., Inc.*[115] decided that social media sites such as Facebook could not be considered an ECS because the information was not privately held but put on public display.[116] However, this court changed views upon reconsideration, holding that the ECS was meant to apply broadly to *any* service that facilitated email communications.[117] The court also indicated that services such as Facebook provide private messaging services.[118] Facebook, therefore, can be classified as more than an ECS but the judge relegated it to one category. By doing so, the court attempted to apply a statute to an area that that it previously recognized was not suited for new technologies like social media.[119] Regardless, the court did not find evidence that the information was available to the public as dispositive.[120] The fact that the information stored on Facebook was held in backup as storage for both the benefit of the user and the ISP allows social media to be categorized within the ECPA.[121]

---

[111] *Id.*
[112] *Id.* at 730.
[113] 717 F. Supp. 2d 965, 977 (C.D. Cal. 2010).
[114] *Id.*
[115] 529 F.3d 892 (9th Cir. 2008).
[116] *Crispin*, 717 F. Supp. 2d. at 980.
[117] *Id.*
[118] *Id.*
[119] *Id.* at 988.
[120] *Id.* at 990.
[121] *Id.*

B. Cases Where SCA Did Not Apply

In the case of *Casillas v. Cypress Insurance Co.*[122] the plaintiffs were unable to obtain relief because the Ninth Circuit held that the SCA did not apply.[123] The plaintiffs, Hector Casillas and Adela Gonzales, stored their worker's compensation information on the defendant's website, which was maintained by a third party called HQSU.[124] The plaintiffs' information was accessed by the defendant, the website creator, at the behest of insurance investigators.[125] The plaintiffs sued in the District Court for the Central District of California, but their complaint was dismissed for failure to state a claim for which relief can be granted.[126] The Ninth Circuit affirmed the district court's judgment denying them relief.[127] It held that the website did not fit into the category of ECS, because the website's users could not communicate directly with one another.[128] Ninth Circuit precedent held that websites that allowed users to communicate with one another were permitted categorization as ECS providers.[129] In analyzing the website in the *Casillas* case, the court stated that the plaintiffs had to download the documents they requested from the server, rather than from another user acting as a sender.[130] In addition, the court recognized that the documents and comments did not travel directly from the sender to the recipient.[131] Therefore, the plaintiffs could not allege that a direct communication occurred.[132] As a result, the website did not receive classification as an ECS and the plaintiffs were denied relief.[133]

In *Cousineau v. Microsoft Corp.*[134] the United States District Court for the Western District of Washington denied the plaintiff

---

[122] 770 Fed. App'x 329, 330 (9th Cir. 2015).
[123] *Id.*
[124] Casillas v. Berkshire Hathaway Homestate Companies, CV 15-04763 (JEMx), 2017 WL 2813145 at *1 (C.D. Cal. 2017).
[125] *Id.*
[126] 770 Fed. App'x at 330.
[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] *Id.*at 331.
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] 6 F. Supp. 3d 1167 (W.D. Wash. 2014).

relief under the SCA[135] because smartphones were classified as ECS.[136] The plaintiff sued the manufacturer for collecting data relating to the user's geographic location through its smartphone.[137] The court analyzed the SCA, but came across a problem when it reached the question of whether mobile phones are facilities.[138] Despite the SCA's not defining a "facility," the court began by working with the SCA's definition of an "electronic communication service."[139] The court defined an ECS as any service which provides users with the ability to send or receive wire or electronic communications, and specifically stated that electronic communications consisted of the sending of images, writings, signs and other information.[140] Smartphones were considered electronic services under the Act, but the issue was whether they came within the definition of a facility.[141]

The court held that smartphones did fit within the definition of a facility, stating that the "device enabled the use of the location services rather than providing them."[142] The SCA was meant to protect facilities operated by electronic communications service providers and maintaining electronic storage, not computers that enabled their use.[143] In the present case, the plaintiff's smartphone did not provide other users with geographical information, but received the relevant information from Microsoft.[144] As a result, plaintiff's phone could not be categorized as a server.[145] The fact that the phone both received and sent data did not change that result because almost all smartphones transmit data to service providers.[146] Finally, the court explained that if it accepted the argument that the smartphone sent geographic information, then Microsoft was providing third parties with access to the plaintiff's phone.[147] Thus

---

[135] 18 U.S.C.A. § 2701(a)(1).
[136] 6 F. Supp. 3d at 1170.
[137] *Id.*at 1170.
[138] *Id*. at 1174.
[139] *Id.*
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.* at 1175.
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *Id.*

the court granted the defendant's motion for summary judgment and denied the plaintiff protection.[148]

The outcomes of *Casillas* and *Cousineau* provide examples of parties being denied relief because the facilities which processed the parties' data did not fit within the definitions in the SCA. In the case of *Casillas*, the website in which the plaintiffs stored their data could be categorized as an RCS, but not an ECS, so relief was denied under the SCA.[149] This prevented the plaintiffs from successfully arguing that some services can be both RCS and ECS.[150] In previous Ninth Circuit cases such as *Quon*,[151] this distinction served to completely deny or grant liability under the statute.[152] In *Quon*, the court granted the plaintiffs' demands for relief pursuant to 18 U.S.C. § 2702 (a)(1) because the service that provided the plaintiffs a platform on which to post text messages could be classified as an ECS.[153] In contrast, the court in *Casillas* found for the defendants even though the plaintiffs proved the website could be classified as an RCS because the plaintiffs created it pursuant to 2702(a)(1), which required the website to be identifiable as an ECS.[154]

IV. THE NINTH CIRCUIT AND DATA PROTECTION

The Ninth Circuit, in examining claims brought under the SCA, has attempted to reconcile the statutory text with the reality of the modern internet.[155] Before the SCA, Congress hoped to address the inability of the Fourth Amendment to address invasions of privacy by new technologies with the passage of a new act.[156] The Fourth Amendment regulated a large, growing field and the rapid development of technology revealed the weakness resulting from its age.[157] Thus, Congress enacted the Wiretap Act, but it was limited in scope and was quickly outpaced by technological advances.[158]

---

[148] *Id.*
[149] Casillas v. Cypress Insurance Co., 770 Fed. App'x 329, 330 (9th Cir. 2015).
[150] *Id.*
[151] 529 F.3d 892, 900 (9th Cir. 2008).
[152] *Id*.
[153] *Id.* at 903.
[154] Casillas, 700 Fed. App'x at 331.
[155] Konop v. Hawaiian Airlines, Inc., 302 F.3d. 868, 874 (9th Cir. 2002).
[156] Baker, *supra* note 1, at 81.
[157] *Id*. at 80.
[158] *Id.*

Congress's attempts to amend the act were not successful because the rapid advancement of technology kept outpacing Congress's amendments.[159] The ECPA was enacted in order to address the Wiretap Act's deficiencies by adding amendments, and one of the ECPA's most prominent provisions was the SCA.[160] Thirty years later, it is the only act that addresses information held in storage despite the change in technology.[161]

The SCA has changed little since its enactment in the 1980s and courts have struggled to apply its outdated definitions.[162] The rapid rise of the internet reduced the SCA's usefulness.[163] The SCA's original purpose was to address a crucial turning point for the Fourth Amendment as the internet was created.[164] Specifically, its goal was to address the internet-based privacy violations that can be brought under the Fourth Amendment, such as the unauthorized access to e-mails by a government entity.[165] However, its narrowly tailored mandate meant it could not be used in cases that do not involve violations of the Fourth Amendment.[166]

Even when the SCA applies to an entity, it might not apply to the information being sought.[167] For an ECS, providers are only prohibited from disclosing information that is held in storage.[168] The SCA defines storage as information held in a computer server incidental to the electronic transmission as well as information that is held in a server for the purpose of backup protection.[169] In contrast, an RCS is only prohibited from disclosing information being held in storage or for computer processing by its customers.[170] Neither of these definitions provides for information that was intercepted.[171] The distinctions between the different services and the lack of clarity

---

[159] *Id.*
[160] *Id.*
[161] *Id.* at 82.
[162] Konop v. Hawaiian Airlines, Inc., 302 F.3d. 868, 874 (9th Cir. 2004).
[163] *Id.*
[164] *Id.*
[165] *Id.*
[166] *Id.*
[167] Baker, *supra* note 1, at 87.
[168] *Id.* at 87.
[169] *Id.* at 87-88.
[170] *Id.*
[171] *Id.*

provide even more problems for those seeking to acquire information that is otherwise disclosable.[172]

A. The Ninth's Circuit Current Use of the SCA

The Ninth Circuit continues to use the SCA to solve internet-related problems that have no precedent to anything seen in the 1980s.[173] In *Rainsy v. Facebook, Inc.*,[174] the District Court for the Northern District of California attempted to address the scope of protection afforded to a "like"[175] when used on Facebook and whether the plaintiff who made the "like" could disclose his or her identity.[176] The court stated that giving a "like" on Facebook equates to showing approval of the post, constituting it as "contents of a communication."[177] Under the SCA, "contents of a communication" concern the substance and meaning of the message.[178] Since revealing the identity concerns the substance of the message, and since the message, the "like," was one of approval, disclosure of the identity of the people who liked the post is precluded.[179]

Another example of the Ninth Circuit using the SCA is presented in the case of *hiQ Labs v. LinkedIn Corporation*.[180] On appeal, the court determined whether an injunction for hiQ Labs, an analytics company, against LinkedIn for invoking the Computer Fraud and Abuse Act (CFAA) was appropriate.[181] In *hiQ Labs*, LinkedIn decided to help employers find the employees they desire by presenting to them the data collected from LinkedIn's servers.[182] The data collected by LinkedIn was present in its servers as a result

---

[172] *Id.*
[173] hiQ Labs v. LinkedIn Corp., 938 F.3d 985, 992 (9th Cir. 2019); Rainsy v. Facebook, Inc., 311 F. Supp. 3d 1101, 1106 (N.D. Cal. 2018); In re Zynga Privacy Litig., 750 F.3d 1098, 1105 (9th Cir. 2014).
[174] 311 F. Supp. 3d 1101, 1114 (N.D. Cal. 2018).
[175] Kari Paul, *Does the 'Like' Mean Anything Anymore?*, N.Y. INTELLIGENCER (May 5, 2016), https://nymag.com/intelligencer/2016/05/does-the-like-mean-anything-anymore.html.
[176] Rainsy v. Facebook, Inc., 311 F. Supp. 3d 1101, 1114 (N.D. Cali. 2018).
[177] *Id.*
[178] *Id.*
[179] *Id.*
[180] 938 F.3d 985 (9th Cir. 2019).
[181] *Id*. at 992.
[182] *Id.* at 991.

of its nearly 500 million users.[183] Previously, hiQ Labs was "data scraping" LinkedIn's servers.[184] Data scraping is the process of using automated bots and algorithms to mine other company's websites for data, which here was LinkedIn, categorize that data and sell it to business clients.[185] Once LinkedIn became aware of hiQ Labs' activities, it sent a cease and desist letter alleging that by data scraping its website, hiQ Labs violated the CFAA.[186]

The lower court granted hiQ Labs' preliminary injunction and LinkedIn appealed.[187] Although the Ninth Circuit relied primarily on the CFAA, it mentioned the SCA. Specifically, it stated that the similarities between the SCA and the CFAA made it clear that the court should interpret the two statutes *pari passu*, or on an equal footing.[188] The court noted the similar language, particularly in a provision from both statutes that stated if anyone were to access information from an electronic communications service without authorization, the accessor would be punished.[189]

The Ninth Circuit's decision in *Konop* remains the standard for cases concerning websites where electronic information is on a "wall," even though that case dealt with electronic bulletin boards years before social media.[190] The Ninth Circuit denied relief under the SCA, holding that Hawaiian Airlines' use of the website was not at the standard required by the SCA.[191] Since social media platforms like Facebook share similar purposes, they too should be governed by this standard.[192] Comparing Facebook's format to the online bulletin in *Konop* is similar to the issue with the SCA as a whole; it does not serve its purpose anymore. In *Konop*, the messages sent to the bulletin board had to be opened to be accessed, while Facebook posts are readily visible to authorized users.[193] As a result, there is no step where a Facebook post is held in storage as were the posts in *Konop*. This lack of compatibility illustrates the foundational issues that the

[183] *Id.*
[184] *Id.*
[185] *Id.*
[186] *Id.*
[187] *Id.*
[188] *Id.* at 1002.
[189] *Id.* at 1002-03.
[190] Baker, *supra* note 1, at 101.
[191] Konop v. Hawaiian Airlines, Inc., 302 F.3d. 868, 880 (9th Cir. 2002).
[192] Baker, *supra* note 1, at 94.
[193] *Id.* at 101.

Konop test faces when applied to social media cases, and why the Ninth Circuit needs to reconsider its approach. That method can only come about once Congress amends the SCA to address the outdated ECS and RCS categories or repeals it outright and enacts a new statute. Once done so, this solution will provide a way to properly judge social media sites from older mediums that share data such as the electronic bulletin board in *Konop*.

The court relied heavily on the similarities between the CFAA and the SCA in its determination as to whether hiQ Labs was precluded from alleging its claim regarding hiQ Labs' gathering of data.[194] The Ninth Circuit discussed its previous decisions in *Konop* to provide guidance on distinguishing between public and non-public websites.[195] *Konop* and *hiQ* both dealt with websites that contain private information provided by their users that are protected by a username and password combination.[196] In *hiQ*, the court recognized that websites that advertise themselves as confidential deserved protection, while those that are accessible to the public would not be able to impose liability on somebody else for accessing it.[197] Since the information that LinkedIn was seeking to protect was not considered confidential or out of the reach of those hoping to access the data, the court could not hold hiQ Labs liable for accessing it.[198] If an effective statute had been in place, hiQ Labs would be liable for not providing a secure website.

The next case provides an example of the use of the SCA to analyze a complicated matter when an updated statute would have performed better. In the case of *In re Zynga Privacy Litigation*,[199] the Ninth Circuit Court of Appeals held that the plaintiffs could not allege a violation of the SCA against Facebook, the developer Zynga or third parties for receiving the Facebook IDs and URLs contained in the plaintiffs' headers.[200] The Ninth Circuit began its analysis by determining if the HTTP referrer information was applicable to the SCA's provisions.[201] The court searched through precedent as far

[194] *Id.*
[195] *Id.* at 1003.
[196] *Id.*
[197] *Id.*
[198] *Id.*
[199] 750 F.3d 1098, 1105 (9th Cir. 2014).
[200] *Id.*
[201] *Id.*

back as the 1980s to define the meaning of the word "contents."[202] The court found that the statute defines contents as any information that concerns the "substance," "purport," or "meaning" of the communication.[203] The court turned to the dictionary definitions of those words in order to understand Congress's intent.[204] In short, after the court's consideration of those dictionary terms, it defined contents as "a person's intended message to another."[205] Although the information in the header could identify the users, the court interpreted the statute as expressly allowing this: it only prevents disclosure of content from a communication, not personally identifiable information.[206]

The court rejected the plaintiffs' argument that the record information can become content if it is the subject of a communication, but the court did not find this convincing.[207] Using *Pharmatrak* as an analogy, the court stated that the header disclosed information about the user's communication, not the communication itself.[208] The plaintiffs also argued that the URLs could provide contents of a communication rather than record information and violate their privacy under the Fourth Amendment, but again, the court disagreed with their claims.[209] Using the Fourth Amendment, the court held that the recorded information, as it stated in past cases, leaves no reasonable expectation of privacy, but content communication does.[210] The court found it determinative that since the URL information includes only basic identification and address information, not search terms, it could not constitute the content of a communication.[211]

---

[202] *Id.*
[203] *Id.*
[204] *Id.*
[205] *Id.* at 1106.
[206] *Id.* at 1107.
[207] *Id.*
[208] *Id.*
[209] *Id.* at 1108.
[210] *Id.*
[211] *Id.* at 1109.

V. THE IMPORTANCE OF *THEOFEL V. FAREY-JONES*

Plaintiffs, officers of ICA, or Integrated Capital Associates Inc., sued the defendant Farey-Jones.[212] During discovery, the defendant took action to acquire the e-mails from ICA about the case and proceeded to subpoena NetGate, the ISP in charge of holding ICA's emails.[213] NetGate, without consulting with ICA first and at the defendant's insistence, relinquished to Farey-Jones over three hundred emails, some containing personal and sensitive information.[214] In response, the plaintiffs brought this action against Farey-Jones and the attorney, alleging violations of the SCA and the CFAA.[215] The United States District Court for the Northern District of California decided that none of the statutes applied and dismissed the claims, and in response, the plaintiffs appealed.[216] The Court of Appeals for the Ninth Circuit previously dealt with this issue in the case of *Konop v. Hawaiian Airlines, Inc.*, and noted that other circuit courts have dealt with the issue differently.[217] The First Circuit held in a case that access might be unauthorized under the CFAA if it is not in line with the reasonable expectations of the party granting permission.[218] The Second Circuit also held that, in one case, access is unauthorized where that access is not related to the system's intended function.[219] In *Theofel*, the court compared the taking of electronic information to trespass: "[J]ust as trespass protects [people] who rent space in a commercial facility to hold sensitive documents, the [Stored Communications] Act protects users whose electronic communications are in electronic storage with an ISP . . . ."[220]

In taking this approach, the court acknowledged that the defendant would not be held liable if the entry was authorized.[221] However, consent given can be invalidated if it was given through

---

[212] Theofel v. Farey-Jones, 359 F.3d 1066, 1071 (9th Cir. 2004).
[213] *Id.*
[214] *Id.*
[215] *Id.* at 1072.
[216] *Id.*
[217] *Id.*
[218] *Id.*
[219] *Id.*
[220] *Id.* at 1072-73 (citations omitted).
[221] *Id.*

deceit.[222] Consent is invalid if the deceit is so egregious that it goes to the essential nature of the act.[223] The distinction between something minor and something major is best defined by the specific interests that an action for trespass was meant to protect.[224] As the court summarized, "[p]ermission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances."[225] As a result, NetGate's consent to the subpoena order was invalidated by the improper nature of this order.[226] It violated the federal rules and allowed information that would have otherwise remained private to be exposed to another party that took few measures to prepare a proper order.[227]

VI. ARGUMENT: WHY THE SCA NEEDS TO BE AMENDED OR REPEALED

The most effective way to protect consumers from the growing threats to their data from third parties is to revise and amend the SCA and the accompanying statutes.[228] According to one prominent computer law professor, Orin Kerr, the SCA "is dense and confusing, and few cases exist to explain how the statute works."[229] Its classifications proved to be its most fatal flaw; in creating two types of providers, the ECS and the RCS, the SCA failed to provide guidance in cases where the providers did not fit in to these categories or could meet both.[230] The SCA was also limited in scope as it was not "a catch-all statute designed to protect the privacy of stored internet communications."[231] Instead, it was narrowly created to address Fourth Amendment violations.[232] As a result, judges have modified the statute to address areas of the internet the SCA was not

[222] *Id.*
[223] *Id.*
[224] *Id.*
[225] *Id.*
[226] *Id.* at 1074.
[227] *Id.*
[228] Burshnic, *supra* note 12, at 1287.
[229] 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, 1208 (2004).
[230] *Id.* at 1214.
[231] *Id.*
[232] *Id.*

designed to govern.[233] Although the drafters of the statute based the SCA on the internet usages of the time, they did not have the foresight to implement measures in the statute to compensate for the internet's rapid evolution.[234] With certain measures in place, the SCA can be an efficient legislative tool in governing information cases regarding both updated and new technologies.

The SCA only provides minimal protection against the disclosure of emails and other sensitive information to third parties, especially the government.[235] Some stored information can be accessed with very minimal effort while the other party is only required to provide notice and serve a subpoena.[236] In effect, the government can "often compel all opened e-mails from an ISP with a mere subpoena and without meaningful notice—precisely the result the SCA was enacted to avoid."[237] Congress's reasoning behind the lower threshold in 1986 was to safeguard the right of privacy protected under the Fourth Amendment.[238] However, this was meant to accommodate the Supreme Court's understanding of the internet at the time.[239] For example, it adhered to notions that if storage is not accessed for over 180 days, then it is considered abandoned.[240] By anchoring the SCA on the Supreme Court's understanding of the internet back in the 1980s, Congress failed to take into account the shifting importance of the internet in modern times.[241] This also poses the concern about Congress's lack of foresight and the courts' as well; neither did Congress anticipate that technology would develop or anticipate that the SCA's categories would be blurred. Specifically, Congress should have known that ECS and RCS definitions would overlap given that some entities fulfill both roles. Congress also should have anticipated that there would be confusion regarding specific phrases like "intentionally divulge." However, Congress allowed the statute to exist without any significant reform.

---

[233] *Id.* at 1214-15.
[234] *See A Short History of the Internet*, SCIENCEANDMEDIAMUSEUM (Dec. 3, 2020), scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet.
[235] *Id.* at 1233.
[236] *Id.* at 1223.
[237] *Id.* at 1234.
[238] *Id.*
[239] *Id.*
[240] *Id.*
[241] *Id.*

The court in *Crispin* focused its inquiry on the wall posts of sites like Facebook and Myspace by utilizing its distinctions in *Konop*.[242] In *Konop*, the court could not categorize the website used in that case as intermediate storage, but thought that it could be categorized as back-up storage.[243] The issue that complicated matters in *Konop* was that it dealt with a BBS, or a bulletin board service.[244] It could not be categorized under the definition of an ECS because when the post reached the board, it was not in an intermediate stage and pending delivery to another source.[245] However, the court reasoned that since the provider did not delete the post on the wall after it had been sent and read, it constituted storage that could be allocated as back-up storage.[246] Also, because the BBS fulfilled the same purpose as Facebook or Myspace, it could not be differentiated and must presumably be held for back-up purposes.[247] In the end, this reasoning only suggests that "the court was determined to apply the SCA whenever possible and that it was in favor of granting the protection the SCA offers."[248] The SCA could then, as a result, be used whenever somebody posts something onto social media.[249] Although it is tempting to consider the bulletin board of *Konop* as an analogy to social media wall posts, the court's decision is more in line with its agenda to keep following the rigid guidelines of the SCA, interpreting the text to apply for today when it was better suited for the situations of the past.

Finally, in *Cousineau*, the court admitted that it cannot define what the SCA regards as a "facility."[250] Instead, the court relied on precedent relating to computers and smartphones along with the SCA's definition of "electronic communications service."[251] In applying the SCA, the court concluded that since mobile phones could not act similarly to SCA facilities by providing location services in a "server-like" fashion, mobile phones could not

[242] *Crispin*, 717 F. Supp. 2d at 988.
[243] Baker, *supra* note 1, at 101.
[244] *Id.*
[245] *Id.*
[246] *Id.*
[247] *Id.* at 102.
[248] *Id.*
[249] *Id.* at 103.
[250] Cousineau v. Microsoft Corp., 6 F. Supp. 3d 1167, 1174 (W.D. Wash. 2014).
[251] *Id*. at 1175.

constitute an ECS.[252] Even when evidence was presented that the mobile device both received and sent out information, the court dismissed the claim, saying that nearly all mobile devices transmit data to service providers.[253] The definitions and standards the Ninth Circuit relied on in using the SCA illustrate the risks and dangers facing potential aggrieved parties as they attempt to seek relief.

VII. CONCLUSION

The plaintiffs in *Theofel* were already involved in litigation when their adversaries, hoping to gain an edge, made aggressive requests in pursuit of discovery that endangered the plaintiffs' privacy.[254] The plaintiffs were able to recover for the damages their adversaries cost them because the court held, based on its interpretation of the SCA, that the defendant's knowledge of the invalidity of the subpoena evidenced knowledge of bad faith and negligence.[255] However, many parties that have had their confidential information accessed under false guises of authorization were not as lucky. To better safeguard the private information of the people, the SCA and the ECPA need to be amended to better conform to the people's expectations for digital security.

The SCA is based on technology from the 1980s and this creates confusion if it is amended. Instead, it should be restructured to account for modern technology. As previously noted, the SCA and ECPA were both created at a time soon after the advent of the internet and have not been updated since.[256] The statutory language does not provide suitable guidelines. Specifically, trying to categorize certain services that provide electronic or wired services between RCS or ECS has created confusion and uncertainty. These categories do not consider entities that can be classified as RCS or ECS. Further complicating matters is that the courts continue to utilize the SCA and work within its archaic categories since Congress has yet to update the statute to address new technologies.[257]

---

[252] *Id.*
[253] *Id.*
[254] Theofel v. Farey-Jones, 359 F.3d 1066, 1071 (9th Cir. 2004).
[255] *Id.* at 1074.
[256] Burshnic, *supra* note 12, at 1261.
[257] *Id.* at 1264.

An alternative to outright repeal of the SCA would be to amend it to better accommodate internet advances. The Ninth Circuit along with other circuits has grown familiar with the SCA over the past three decades.[258] Without action from Congress, the Ninth Circuit has had little choice but to continue using the Act in response to the growing number of cases that involve information online and through platforms like social media. However, courts have struggled to apply the SCA. The various ways that information is being shared between users and companies use their users' information to benefit their subscribers as well as themselves are scenarios to which the SCA will likely never adapt. If the statute were to be repealed, courts would have to spend years learning new definitions that would surely be more complicated than the SCA is today. There is also the chance that case law might be overturned should new amendments to the SCA be introduced. However, amending the SCA would allow the law to conform to modern standards without creating the shock that would come with repealing the statute outright. The creators of the SCA had good intentions, but the SCA of the future or a similar equivalent should be enacted or amended to consider the ever-changing use of technology.

[258] The First Circuit looked towards the reasonable expectations of the party granting permission in making their judgment in one case, while the Second Circuit focused on whether the party's access was related to the system's intended function. Theofel v. Farey-Jones, 359 F.3d 1066, 1072 (9th Cir. 2004).