Privy or Private: A New Age Look at Old School Privacy Laws

Carlos Aguilar

Follow this and additional works at: http://scholarlycommons.law.cwsl.edu/cwlr

Recommended Citation
Available at: http://scholarlycommons.law.cwsl.edu/cwlr/vol53/iss1/8
COMMENT

PRIVY OR PRIVATE: A NEW AGE LOOK AT OLD SCHOOL PRIVACY LAWS

TABLE OF CONTENTS

PROLOGUE .................................................................................................................. 86
I. INTRODUCTION ........................................................................................................ 88
II. FOURTH AMENDMENT JURISPRUDENCE ............................................................ 90
   A. From a Physical Trespass to a Reasonable Expectation of Privacy ................. 91
   B. The Third-Party Doctrine .................................................................................. 93
III. THE STORED COMMUNICATIONS ACT: A STATUTORY FRAMEWORK .............. 95
   A. Electronic Communication Service & Remote Computer Service Dichotomies .............. 96
   B. Title 18 U.S.C. Section 2703 ........................................................................ 98
IV. THE SCA, FOURTH AMENDMENT, & TECHNOLOGY ........................................ 100
   A. Email Technology ............................................................................................ 101
   B. Cellphone Tracking ....................................................................................... 104
V. A NEW DIRECTION FOR FOURTH AMENDMENT JURISPRUDENCE ................. 108
   A. The Validity of Equilibrium-Adjustment .............................................................. 109
   B. The Privacy of Our Information ........................................................................ 113
   C. The Privacy of Our Movements ....................................................................... 115
   D. Modernizing the Third-Party Doctrine ............................................................... 116
VI. THE PROPOSED REVISION FOR THE STORED COMMUNICATIONS ACT ............ 118
   A. California Electronic Communication Privacy Act of 2016 ............................. 118
   B. Requiring a Search Warrant Creates Proper Transparency ......................... 119
CONCLUSION .............................................................................................................. 121

85

http://scholarlycommons.law.cwsl.edu/cwlr/vol53/iss1/8
PROLOGUE

November 13, 2015, was a beautiful winter night in Paris—or, at least it started out that way.¹ Thousands of spectators attended the football match between Germany and France at the Stade de France.² The American rock band Eagles of Death Metal was playing in front of hundreds of fans in the Bataclan Concert Hall³ while other residents and tourists went out to enjoy the bars and restaurants around the famed “City of Light.”⁴ Shortly after nine o’clock, a large explosive was detonated outside the Stade de France.⁵ Islamic terrorists commenced a series of coordinated and violent attacks upon the heart of France’s capital killing 130 people.⁶ By eleven o’clock, Paris was under a state of emergency.⁷ A beautiful winter night in Paris transformed into a night of unimaginable horror.⁸

Meanwhile, in the United States, CIA director John Brennan pressures Congress to increase government surveillance.⁹ The recent terrorist attacks in Paris and San Bernardino,¹⁰ renewed a debate on how

---

². Id.
³. Id.
⁴. See id.
⁵. Id.
⁶. Id.
⁷. Id.
⁸. See generally id.
to balance Americans’ privacy interests with the importance of national security.\textsuperscript{11}

Based on these security concerns, the desire for new surveillance programs in the United States seems rational; however, it should be noted that the French Surveillance Bill “did nothing to stop [the Paris] attacks.”\textsuperscript{12} In May 2015, the French National Assembly voted to expand its already comprehensive surveillance operation due to the terrorist attack that occurred months earlier.\textsuperscript{13} These additional provisions authorized intelligence services to monitor phone calls and emails without a warrant.\textsuperscript{14} Increasing government surveillance similar to the French Surveillance Bill presents scenarios that implicate the Fourth Amendment.\textsuperscript{15} James Madison said it best:

\begin{quote}
Since the general civilization of mankind, I believe there are more instances of the abridgment of freedom of the people by gradual and silent encroachments by those in power than by violent and sudden usurpations. On a candid examination of history we shall find that turbulence, violence, and abuse of power by the majority trampling on the rights of the minority, have produced factions and commotions, which in republics, have more frequently than any
\end{quote}

\textsuperscript{11} See Tom McCarthy, \textit{Surveillance Must Increase After Terror Attacks, Say 2016 Candidates}, \textit{The Guardian} (Dec. 6, 2015, 1:07 PM), http://www.theguardian.com/us-news/2015/dec/06/paris-attacks-san-bernardino-shooting-surveillance-hillary-clinton-donald-trump-election. Presidential candidate Hilary Clinton agreed that new government surveillance is needed, but also understood that “[n]obody wants to be feeling like their privacy is invaded.” \textit{Id}. In contrast, Donald Trump wanted to increase government surveillance that includes tracking entire families and maintain a database on American Muslims. \textit{Id}. Jeb Bush described Trump’s suggestion as “abhorrent” because the United States has all the capability “to monitor people that are in our country trying to attack us.” \textit{Id}.

\textsuperscript{12} Peterson & Fung, \textit{supra} note 9 (noting that France’s new bill was unable to prevent the recent Paris attacks).


\textsuperscript{14} See Rubin, \textit{supra} note 13.

\textsuperscript{15} See U.S. CONST. amend. IV.
other cause produced despotism. If we go over the whole history of the ancient and modern republics, we shall find their destruction to have generally resulted from those causes.  

I. INTRODUCTION

Thirty years ago, the Stored Communications Act ("SCA") was enacted to regulate and monitor government procedures used to compel electronic stored information from its citizens. Privacy advocates hotly opposed the statute for authorizing warrantless access to emails and tracking cellphones using cell site location data. Scholars and legal professionals alike are quick to point out that the SCA's warrantless access to electronic stored information violates the Fourth Amendment, and is incompatible with the advances of modern technology.


The dispute behind warrantless access to emails and cell site location data is critical because current Fourth Amendment jurisprudence is inadequate to protect electronic stored information. This inadequacy stems from emails and cell site location data being stored on equipment owned by a private service provider, thus invoking the third-party doctrine—an exception to the warrant requirement.

Indeed, the federal government’s capability to monitor emails and track cellphones without a warrant is the type of “gradual and silent encroachment” James Madison foreshadowed. Current public opinion shows people believe their government could do more to ensure their privacy interests. These searches violate the Fourth Amendment, primarily because they occur without a warrant, but also because they reveal intimate and sensitive information about an individual. Thus, the SCA should be amended because the language and its application are plagued with legal fallacies that implicate the Fourth Amendment and fail to adequately adjust to modern technology.

This Comment proposes that Congress amend the SCA, or at minimum, enact legislation that affords digital privacy protections that require a probable cause showing. New or amended privacy legislation would enhance the public’s perception of their government because it would protect people’s privacy interests and provide clear guidance for law enforcement officers. Part II provides background information about Fourth Amendment jurisprudence. Part III describes the SCA’s


20. See In re United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013); Rehberg v. Paulk, 611 F.3d 828, 846-47 (11th Cir. 2010).

21. See cases cited supra note 20; see also discussion infra Section II.B, III.A-B.


24. See U.S. CONST. amend. IV.

statutory framework. Part IV applies the SCA to emails and cell site location data to demonstrate its inadequacy to uphold Fourth Amendment protections, including the privacy implications of evolving technology. Part V analyzes United States Supreme Court precedent using Professor Kerr’s equilibrium-adjustment theory to provide an alternative solution to protect emails and cell site location data. Finally, Part VI proposes that Congress amend the SCA’s statutory framework, and follow California’s Electronic Communications Privacy Act of 2016 provisions for law enforcement to obtain electronic stored information.

II. FOURTH AMENDMENT JURISPRUDENCE

The historical context behind unreasonable searches was to protect against arbitrary and intrusive invasions. This apprehension dates back before the country was founded, when American colonists opposed British custom officials who used general writs of assistance. The writs of assistance authorized British officers to arbitrarily rummage through houses without restrictions looking for any evidence of criminal activity. The colonists’ opposition to these searches was one primary reason behind the Revolutionary War. Accordingly, when those same colonists won their independence they desired a law that prevented those kinds of intrusions from occurring in their new nation. The Fourth Amendment provided for “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, and [that] no warrant shall issue


27. See Nelson B. Lassen, The History and Development of the Fourth Amendment to the United States Constitution 56 (1937). These writs of assistance authorized British custom officials to conduct indiscriminate searches that remained effective during the sovereign’s lifetime. Id.

28. Id. at 54.

29. Id. at 51. The author discusses three separate occasions about how Britain’s use of writs of assistance created a chain of events that led to the Declaration of Independence and the American Revolutionary War. See generally id. at 56-73.

30. See id. at 51.
but upon probable cause by Oath or affirmation . . . .” Therefore, warrantless searches are unreasonable—subject to a few exceptions.  

A. From a Physical Trespass to a Reasonable Expectation of Privacy

From the Fourth Amendment’s ratification in 1791 until 1967, a search inquiry was limited to a physical trespass against an individual’s constitutionally protected area. Yet, as technology progressed, limiting the amendment’s protection to only a physical trespass search created problematic situations.  

In *Olmstead v. United States*, the United States Supreme Court addressed whether installing a wiretap on a person’s home telephone without a warrant violated the Fourth Amendment. The Court held that no search occurred because the telephone conversation was intercepted without entering defendant’s property. Justice Brandeis criticized the majority decision for failure to take into account the technological advancements at the time. Instead, the majority’s

31. U.S. CONST. amend. IV.  
32. *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971); *see, e.g.*, *United States v. Ross*, 456 U.S. 798, 808-09 (1982) (holding that a warrantless search against a person’s vehicle is allowed only if there is probable cause to search); *United States v. Santana*, 427 U.S. 38, 42-43 (1976) (holding that exigent circumstances arise when officers are chasing a criminal suspect in a hot pursuit from a public place onto a private residence); *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (consenting to searches results in a legal search that overrides the need for a search warrant and probable cause).  
35. *Id.*  
36. *Id.* at 455. There, officers discovered that defendant was operating a successful bootlegging business. *See id.* at 455-57. At the time, the United States outlawed the possession, importation, or transportation of intoxicating liquors. U.S. CONST. amend. XVIII, § 1, *repealed by U.S. CONST. amend. XXI.*  
37. *Olmstead*, 277 U.S. at 466.  
rationale was based upon a narrow construction of the Fourth Amendment’s language. As Justice Brandeis noted, the Fourth Amendment is much broader in scope and must evolve with the “progress of science,” rather than diminish an individual’s privacy interest.

Following the Olmstead decision, the Court continued to strictly apply a trespass analysis. By 1967, almost forty years later, the Court finally deviated from its strict literalist approach emphasized under Olmstead. In Katz v. United States, FBI agents installed a wiretap outside a public phone booth. The Court recognized that a person who enters a phone booth and shuts the door to make a private phone call deserves constitutional protection. This is because the “Fourth Amendment protects people, not places.” As such, the Court formulated a new and separate Fourth Amendment search inquiry: (1) whether an individual subjectively exhibits an expectation of privacy in the places, containers, or effects searched; and (2) whether society objectively recognizes that expectation of privacy as reasonable. Thus, arose the reasonable expectation of privacy test.

1920/ (discussing significant technological innovations within the first part of the twentieth-century).

39. See Olmstead, 227 U.S. at 476 (Brandeis, J., dissenting).
40. See id. at 474, 478.
41. See, e.g., Silverman v. United States, 365 U.S. 505, 509-12 (1961) (holding that a warrantless use of a spike mike installed against a heating duct at defendant’s house to overhear a conversation was a physical trespass). But see Goldman v. United States, 316 U.S. 129, 134-36 (1942) (holding that a warrantless use of a detectaphone installed at defendant’s adjoining office without penetrating his wall was not a physical trespass).
42. See Katz v. United States, 389 U.S. 347, 353 (1967). A strict literalist approach is interpreting the Fourth Amendment under property law concepts that limits Fourth Amendment protections to only physical intrusions, rather than a person’s tangible item. Thomas K. Clancy, What is a “Search” Within the Meaning of the Fourth Amendment?, 70 ALB. L. REV. 1, 17 (2006).
44. Id. at 348. FBI agents recorded defendant’s conversation that revealed his involvement with illegal interstate gambling. Id.
45. Id. at 352.
46. Id. at 351.
47. See id. at 361 (Harlan, J., concurring).
48. Id.
B. The Third-Party Doctrine

Whether an individual maintains a reasonable expectation of privacy depends upon "[w]hat [that] person knowingly exposes to the public."\(^{49}\) This is because a person loses any reasonable expectation that information voluntarily shared with a third party will remain private.\(^{50}\) The third-party doctrine developed from cases involving defendants disclosing their illegal activities to an informant or an undercover agent.\(^{51}\) The Fourth Amendment does not protect a person's misplaced confidence that a third party will not reveal the communicated illegal activity.\(^{52}\) The United States Supreme Court and lower courts have applied the third-party doctrine broadly.\(^{53}\)

In *United States v. Miller*,\(^{54}\) the Court found the defendant had no privacy expectations in his bank account records.\(^{55}\) Despite the defendant's assumption that his financial records would be used for a limited purpose, he was unable to claim an interest in "ownership []or possession."\(^{56}\) Instead, the bank had possessory interest over the defendant's account records because the financial documents were used during "the ordinary course of business."\(^{57}\) When the defendant

\(^{49}\) Id. at 351 (majority opinion).


\(^{52}\) Hoffa, 385 U.S. at 302.


\(^{55}\) Id. at 444-45. There, the government subpoenaed defendant's bank, which revealed his involvement in an illegal whiskey distillery. *Id.* at 437-38.

\(^{56}\) See *id.* at 440. Here, the defendant had no privacy interest over his financial records suggests that he lacked any standing. *See id.* at 440-41; see also Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) (explaining that standing focuses on the person challenging the illegality of a search and whether that person has any privacy interest in the area searched).

\(^{57}\) Miller, 425 U.S. at 442-43.
voluntarily turned over his financial documents to the bank, he assumed
the risk that the bank would turn these over to the government. 58

Similarly, in Smith v. Maryland, the Court applied the third-party
doctrine to telephone numbers dialed. 59 Without a warrant, officers
used a pen register that revealed the defendant had recently committed
a robbery and made criminal threats against his victim. 60 In applying
Katz, the Court found that unlike a wiretap, a pen register only reveals
telephone numbers dialed, and not the contents of a telephone
conversation. 61 As in Miller, the defendant lacked any privacy
expectations because he voluntarily conveyed the phone numbers
dialed to the telephone company within the “ordinary course of
business.” 62 As such, defendant assumed the risk because he should
have known that all phone numbers dialed are transmitted to the
telephone company. 63 Scholars and legal practitioners alike have
heavily criticized these decisions applying the third-party doctrine. 64

According to critics, judges who cannot recognize bank records and
phone records as being entitled to a reasonable expectation of privacy
are out of touch with society. 65 From a practical standpoint, in a
contemporary society people expect their financial records to remain
confidential because banks are an essential component of a market
economy. 66 As Justice Marshall pointed out, unless society is willing to
relinquish personal or professional necessities, “[i]t is idle to speak of
‘assuming’ the risks in context where, as a practical matter, individuals
have no realistic alternative.” 67

58. See id. at 443-44.
60. Id. at 737. A pen register records numbers dialed on a telephone through
electrical impulses each time a number is dialed. Id. at 736 n.1.
61. Id. at 741.
62. Id. at 744-45.
63. Id. at 742.
64. Kerr, Third-Party, supra note 50, at 563 n.5, 564 (citing to numerous books
and articles that criticized the third-party doctrine). Professor Orin Kerr describes the
third party doctrine as the Lochner to Fourth Amendment jurisprudence. Id. at 563. It
is the “rule scholars love to hate.” Id.
65. Id. at 570.
dissenting).
Nonetheless, the decision in Smith called into question the privacy interest in confidential information handed to a third party. As Justice Brandeis foreshadowed, technological innovations have made government intrusion upon a person’s privacy without legal ramifications possible. With the advancements in information technology, Congress recognized that Fourth Amendment protection remained unclear for people’s personal effects left for storage and processing on computers.

III. THE STORED COMMUNICATIONS ACT: A STATUTORY FRAMEWORK

During the 1980’s, existing federal law was unable to keep up with modernized communication, computer technology, and the telecommunication industry. In response, Congress enacted the Electronic Communications Privacy Act of 1986 ("ECPA") to protect against unauthorized seizures of electronic surveillance. ECPA aimed to create a balance between Americans’ privacy expectations and law enforcement interests. Accordingly, ECPA created three governing statutes: (1) the Wiretap Act, (2) the Stored Communications Act, and (3) the Pen Register Statute.

The legislative intent behind the Stored Communications Act ("SCA") was to protect electronic communications stored with Internet Service Providers by incorporating Fourth Amendment like

---

protections. This privacy protection limits the government’s ability to compel an Internet Service Provider to disclose subscriber information. Ultimately, the SCA protects two classes of service providers: electronic communication services and remote computing services providers.

A. Electronic Communication Service & Remote Computer Service Dichotomies

Before describing the procedures for compelling disclosure, a basic understanding about the differences between an electronic communication service ("ECS") and a remote computer service ("RCS") is needed. These differences determine whether a person is entitled to SCA protections.

An ECS is a service that provides users with the capacity to transmit electronic communications. An ECS is most protected while an electronic communication is in electronic storage. Sending an electronic communication enables electronic storage incident to transmission, and the communication is stored for backup purposes.

---

77. See Kerr, SCA Guide, supra note 19, at 1212. An electronic communication is defined as “any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . .” 18 U.S.C.A. § 2510(12) (2012).


80. See id. at 1215. Compare 18 U.S.C. § 2510(15) (defining ECS as “any service which provides to users thereof the ability to send or receive wire or electronic communications”), with 18 U.S.C. § 2711(2) (defining RCS as “the provision to the public of computer storage or processing services by means of electronic communications systems”).


82. 18 U.S.C. § 2510(15).

83. See id. § 2703(a); see also id. § 2510(17)(A)-(B) (defining electronic storage as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of back up protection of such communication”).

84. See id. § 2510(17)(A)-(B); UNITED STATES DEP’T OF JUSTICE, PROSECUTING COMPUTER CRIMES 92 (2d ed. 2010) [hereinafter PROSECUTING
To provide some context, courts interpret emails as an ECS in electronic storage only when the email is unread as it sits unopened on a service provider awaiting the recipient’s retrieval.85 At this stage, the email is classified as an ECS in electronic storage because the email is stored as a “temporary and intermediate measure pending the recipient’s retrieval of the communication from the service provider.”86

In contrast, an RCS is a provider that offers the public long-term storage services, and computer processing services through electronic communication systems.87 In essence, an RCS acts like a storage facility that stores or processes data to customers (the public).88 A key distinction between an ECS and an RCS is that an RCS must be available to the public.89 An email web service like Gmail is a public provider because any member from the general population could register for an account.90 By contrast, a university that provides students an email account is not considered an RCS because it is limited only to students.91 Yet, electronic communications may also act as both an ECS and RCS or as neither.92

---

85. See, e.g., Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114-15 (3d Cir. 2003) (holding that there was no SCA protection once the emails were read because it was no longer in “temporary, intermediate, storage.”); PROSECUTING COMPUTER CRIMES, supra note 84; Kerr, SCA Guide, supra note 19, at 1216.


88. SEARCHING AND SEIZING, supra note 86, at 119.


90. See id.

91. Id. at 1226.

92. Id. at 1215-16; see, e.g., United States v. Weaver, 636 F. Supp. 2d 769, 770 (C.D. Ill. 2009) (holding that Microsoft’s email service provider offered both ECS and RCS services); In re Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299,
Undoubtedly, courts have difficulty applying modern technology to the SCA because the subtle distinctions between ECS and RCS derive from technology in the 1980’s.\textsuperscript{93}

\textbf{B. Title 18 U.S.C. Section 2703}

Title 18 of United States Code section 2703 regulates how the government may compel a service provider to disclose a subscriber’s electronic communications.\textsuperscript{94} Section 2703 creates different privacy protections for electronic communications in an ECS and those in an RCS.\textsuperscript{95} To access ECS content information, a government must obtain a warrant based upon probable cause only if the content information is in electronic storage for less than 181 days.\textsuperscript{96} After 180 days, a warrant is no longer required.\textsuperscript{97}

Instead, after 180 days, the government may use a process less stringent than a warrant, so long as the subscriber receives prior notice.\textsuperscript{98} The government may access ECS content information stored over 180 days, including RCS content information, using either a court order or a subpoena.\textsuperscript{99} Furthermore, a request for ECS and RCS non-content information does not require notice to the subscriber.\textsuperscript{100}

\begin{tabular}{l}
\textsuperscript{93} See Kerr, SCA Guide, supra note 19, at 1213. Courts analyzing the SCA have described it as a “complex, often convoluted area of the law.” United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) (describing the unfortunate task of conducting a legal analysis on the SCA because it is a “complex, often convoluted” area of law); see United States v. Councilman, 418 F.3d 67, 80 (1st Cir. 2005) (citations omitted); United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003) (citations omitted); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (7th Cir. 2002) (citations omitted). \\
\textsuperscript{94} See 18 U.S.C. § 2703 (2012). \\
\textsuperscript{95} Id. § 2703(a)-(b). \\
\textsuperscript{96} Id. § 2703(a); see also FED. R. CRIM. P. 41(d) (describing the procedures to obtain a warrant). \\
\textsuperscript{97} See 18 U.S.C. § 2703 (a)-(b). \\
\textsuperscript{98} See id. § 2703(b)(1)(B). \\
\textsuperscript{99} Id. § 2703(b)(1)(B)(i)-(ii). An RCS does not require a warrant regardless of whether an electronic communication has been stored less than 180 days. See id. § 2703(b). \\
\textsuperscript{100} Id. § 2703(c)(3).
\end{tabular}
A NEW AGE LOOK AT OLD SCHOOL PRIVACY LAWS

Content information is classified as basic subscriber information or other non-content information. Access to basic subscriber information merely requires an administrative subpoena that reveals a subscriber’s name, address, and telephone records. Access to other non-content information requires a warrant, a court order, or the subscriber’s consent.

Content information is afforded the greatest protection because it includes an electronic communication’s substance. Within the context of emails, the actual text in the email’s body is content information, including the subject line because it carries a substantive message. By contrast, non-content information that is basic subscriber information is deemed less private because the subscriber’s name, address, and telephonic records are knowingly exposed to the service provider. Other non-content information includes account usage records; cell site location data; email headers, excluding the subject line; Internet Protocol addresses; and list of outgoing email addresses.

102. 18 U.S.C. § 2703(c)(2). Other basic subscriber information includes subscriber’s address, length of service with the provider, and payment records. Id.
103. Id. § 2703(c).
104. See id. § 2510(8) (defining the contents of electronic communication as “any information concerning the substances, purport, or meaning of that communication”). Compare id. § 2703(b)(1)(B) (requiring notice to a subscriber if the electronic communication is content information), with id. § 2703(c)(3) (requiring no notice to the subscriber if the electronic information is non-content information). Cf. Warshak v. United States, 631 F.3d 266, 288 (6th Cir. 2010) (holding that a subscriber is entitled to “a reasonable expectation of privacy to the contents of [his] emails”).
106. See 18 U.S.C § 2703(c)(2)(A)-(F); see also Katz v. United States, 389 U.S. 347, 351 (1967) (stating that “[w]hat a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection.”). Subscriber information is knowingly exposed to a service provider because when a person registers for an email account or purchases a cellphone that specific individual voluntarily provides his name, address, and other basic information about himself. See, e.g., Create your Google Account, https://accounts.google.com/SignUp (last visited Oct. 19, 2016) (creating an email account for Google requires providing your first and last name, date of birth, and mobile phone number).
107. Kerr, SCA Guide, supra note 19, at 1228; see also In re United States for Historical Cell Site Data, 724 F.3d 600, 605-06 (5th Cir. 2013) (describing cell site location data as non-content information); United States v. Forrester, 512 F.3d 500,
Alternatively, the government may avoid providing prior notice to a subscriber up to ninety days in the interests of justice. Subsequent delay may be extended for an additional ninety days. In doing so, however, a court must find a reason to believe prior notice may cause an adverse result. An adverse result is similar to that required under the Fourth Amendment’s exigent circumstances, and includes risks of serious bodily injury or death, flight, destruction of evidence, threatening witnesses, and jeopardizing investigations. Ultimately, a government entity has flexibility to compel disclosure of an individual’s email or cell site location data.

IV. THE SCA, FOURTH AMENDMENT, & TECHNOLOGY

Nearly thirty years later, the SCA is incompatible with modern technology because technology has developed significantly since the 1980’s. The SCA was enacted with a noble purpose: to incorporate Fourth Amendment like protections that might be subject to control under the third-party doctrine. Yet, it ironically sets a low threshold for the government to obtain electronic communications. Section 2703(d) reflects Terry v. Ohio’s reasonable suspicion standard, a

510 (9th Cir. 2007) (holding that the “to” and “from” addresses on emails does not amount to reasonable expectations of privacy because it is non-content information).
109. Id. § 2705(a)(4).
110. Id.
111. Id. § 2705 (a)(2).
112. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (7th Cir. 2002) (noting that “until Congress brings the laws in line with modern technology, protection of the Internet and websites such as Konop’s will remain a confusing and uncertain area of law”). See generally Steve Almasy, The Internet Transforms Modern Life, CNN (Oct. 10, 2005, 2:00 PM), http://www.cnn.com/2005/TECH/internet/06/23/evolution.main/ (discussing the Internet’s impact on society).
114. See 18 U.S.C. §§ 2703 (a)-(d).
115. Terry v. Ohio, 393 U.S. 1, 21-22, 28 (1968) (holding that officers are authorized to temporarily seize a person based upon “specific and articulable facts which, taken together with rational inferences from those facts” establish reasonable suspicion that criminal activity is afoot).
standard lower than probable cause. In essence, it merely requires a short factual summary describing the criminal investigation and how the electronic communication would help further the investigation’s interest. This defeats the whole purpose behind the SCA’s enactment. Like the Fourth Amendment, the SCA should require a warrant based upon probable cause to access emails and cell site location data.

A. Email Technology

The SCA permits the government to obtain emails under 18 U.S.C. § 2703(a)-(b). A basic understanding of emails is necessary to understand why the SCA is incompatible with modern email systems. The technology that currently enables a computer to communicate with an email server is the Simple Mail Transfer Protocol (“SMTP”). In 1986, the email server used for retrieving outgoing mail was the Post Office Protocol (“POP”). The POP downloaded every email and

116. United States v. Perrine, 518 F.3d 1196, 1201-02 (10th Cir. 2008). Probable cause requires that law enforcement show that there is evidence of a “fair probability” or a “substantial chance of discovering evidence of criminal activity.” Safford Unified Sch. Dist. #1 v. Redding, 557 U.S. 364, 371 (2009) (citations omitted). In contrast, reasonable suspicion requires a moderate chance to find evidence of criminal activity. Id. Thus, reasonable suspicion is “obviously less demanding” than probable cause. United States v. Sokolow, 490 U.S. 1, 7 (1989).

117. SEARCHING AND SEIZING, supra note 86, at 131. The Third and Fifth Circuit courts have analyzed the SCA’s plain language and legislative history to determine whether a magistrate judge has the discretion to deny access to cell site location data upon a showing of reasonable suspicion. Compare In re United States for Historical Cell Site Data, 724 F.3d 600, 607 (5th Cir. 2013) (holding that SCA’s section 2703(d) requires a magistrate judge to issue a court order upon a showing of reasonable suspicion), with In re United States for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t, 620 F.3d 304, 313 (3d Cir. 2010) (holding that SCA’s section 2703(d) authorizes a magistrate judge to exercise its discretion whether to require a warrant based upon probable cause or require a showing of reasonable suspicion to access cell site location data).

118. See U.S. CONST. amend. IV.


120. See Achal Oza, Amend the ECPA: Fourth Amendment Protection Erodes as Email Gets Dusty, 88 B.U. L. Rev. 1043, 1052 (2008).

121. Id.; see also Email Basics: POP3 Is Outdated; Please Switch to IMAP Today, HOW-TO GEEK, http://www.howtogeek.com/197207/email-basics-pop3-is-outdated-please-switch-to-imap-today/ (last visited April 6, 2016) [hereinafter Email Basics].
saved it onto a computer because the POP’s megabyte had limited space for email storage. In essence, emails sent in the 1980’s were fragmented because the process involved transferring the email from server to server, and storing it at different locations, before the message was actually downloaded onto a computer. Today, modern emails have a high storage capacity and often sync with a webmail account service like Gmail.

To provide some context why the SCA’s email protection is incompatible with modern email systems, imagine an email is sent to a Gmail account. While the email is unread and awaiting the recipient’s retrieval, the email is most protected because it is classified as an ECS in electronic storage. If the email remains unread for 180 days or more, the government is required to obtain a warrant to retrieve and read the email. However, once the recipient reads the message, the email is no longer classified as an ECS in electronic storage. Instead, the email is classified as an RCS, and no warrant is required because the message is stored on Google’s server. The only way to protect an email from a warrantless search is to never read the message or download it onto a personal computer. This is impractical because technology has changed the way people access their emails, as compared to 1986.

To date, the United States Supreme Court has yet to address whether an email is entitled to Fourth Amendment protection. But, there is no reason to treat emails any different from a telephone conversation or postal mail. Despite the third-party doctrine, the United States

122. Emails Basics, supra note 121.
123. See Oza, supra note 120, at 1051-53; Emails Basics, supra note 121.
124. See Oza, supra note 120, at 1072-73; Emails Basics, supra note 121.
125. PROSECUTING COMPUTER CRIMES, supra note 84; Kerr, SCA Guide, supra note 19, at 1216.
126. See 18 U.S.C. § 2703(a) (2012); see also sources cited supra note 85.
127. SEARCHING AND SEIZING, supra note 80, at 124; Kerr, SCA Guide, supra note 19, at 1216.
129. See generally id.
130. See Oza, supra note 120, at 1073.
Court of Appeal for the Sixth Circuit held that an email’s content is entitled to Fourth Amendment protection. 132

Although emails are stored with a third-party server, the Sixth Circuit found that email communications were different from the bank records in United States v. Miller, and the phone records in Smith v. Maryland. 133 This is because a service provider merely acts as an intermediary. 134 Similar to a telephone company or a postal office, a service provider only delivers and stores an email’s message to the recipient’s server. 135 The Sixth Circuit reasoned that the “Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.” 136 Emails are the “technological scion of tangible mail” that has become an essential means of communication. 137 It would defy contemporary standards of living to deny emails Fourth Amendment protection. 138 Thus, the Sixth Circuit court found SCA’s warrantless access to an email’s contents unconstitutional. 139

Following Warshak, several courts agreed that individuals have a reasonable expectation of privacy in the contents of electronic information. 140 Yet, in other jurisdictions, without an amended statute or a United States Supreme Court decision, there is no deterrence to

132. Warshak v. United States 631 F.3d 266, 288 (6th Cir. 2010).
133. Id. at 287-88; see supra Section II.B.
134. See Warshak, 631 F.3d at 288.
135. Id. at 286-88.
136. Id. at 285.
137. Id. at 286.
138. See id.
139. Id. at 288.
officers accessing emails without a warrant. Ultimately, those defendants may be denied an exclusionary rule remedy.

**B. Cellphone Tracking**

Within the SCA, the government may access cell site location data under 18 U.S.C. § 2703(c). Section 2703(c) treats cell site location data as a non-content communication record. In essence, cell site location data is treated as metadata information. Given that cell site location data constitutes non-content information, the SCA does not require a warrant. Yet, like emails, cellphones are prevalent in contemporary society. To understand what cell site location data actually is, it is important to know how cellphones operate.

Cellphones use radio waves to connect to users’ service providers. Cellular providers preserve a network of radio cell towers

---

141. See Rehberg v. Paulk, 611 F.3d 828, 843-47 (11th Cir. 2010) (noting that the law is unclear whether there is a reasonable expectation of privacy within the contents of emails).

142. See Warshak, 631 F.3d at 289 (holding that defendant was denied an exclusionary remedy due to officers’ good faith reliance upon SCA’s constitutionality). The exclusionary rule is a remedy for a defendant because it excludes evidence of guilt due to a Fourth Amendment violation. But see Illinois v. Krull, 480 U.S. 342, 347 (1987) (explaining that when officers conducted a search based upon reasonable reliance on statutory authority then the exclusionary rule does not serve its purpose); Davis v. United States, 564 U.S. 229 (2011) (holding that “searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule.”)

143. See In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 605-06 (5th Cir. 2013).

144. See 18 U.S.C § 2703(c) (2012).

145. See United States v. DiTomasso, 56 F. Supp. 3d 584, 589-90 (S.D.N.Y. 2014) (describing non-content communication that is incidentally disclosed to third parties as metadata information); see also Klayman v. Obama, 957 F. Supp. 2d 1, 41 (D.D.C. 2013) (indicating that telephony metadata surveillance was likely unconstitutional), vacated, 800 F.3d 559 (D.C. Cir. 2015). This case was vacated on procedural grounds, and no decision was made on the constitutionality of telephone metadata. Klayman v. Obama, 800 F.3d 559, 561 (D.C. Cir. 2015).

146. See 18 U.S.C. § 2703(c).


148. See Electronic Communication Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, and
throughout their coverage areas. A cell site is a specific area near a cell tower containing a wireless antenna that detects the radio signal and spreads from a cellphone and connects to the local cellular network. These radio signals generate cellphone site location data.

Whenever a cellphone makes or receives a call (or sends or receives a text message), the phone connects through radio waves to an antenna located on the nearest cell tower. Accordingly, as individuals go throughout their day, cellphones generate a detail database about their current whereabouts over time. Thus, cellular providers maintain geographic location records on every American who uses a cellphone.

Law enforcement agencies often compel cell site location data from private cell phone providers to track a person's past movements within a geographic area. Just this past year, officers made tens of thousands of requests to mobile carriers for cell site location data. In 2014, AT&T received 64,703 requests, and within the first half of 2015, Verizon received more than 21,000 requests.

While the United States Supreme Court has yet to decide the constitutionality behind cell site location data, there is no certainty

---

*Investigations of the H. Comm. on the Judiciary, 113th Cong. 43 (2013) [hereinafter Geolocation Hearing] (oral testimony of Prof. Matthew Blaze, Univ. of Penn.).

149. Id.

150. Id. at 50 (written testimony of Prof. Matthew Blaze).


152. Geolocation Hearing, supra note 148, at 50 (written testimony of Prof. Blaze).


155. See Meyer, supra note 153.

156. Id.

157. Id.

whether the government could know in advance that cell site location data would reveal sensitive and intimate information about a person. 159

Most recently, federal appellate courts have applied section 2703(d) to cell site location data. 160

The Fourth Circuit found that warrantless access to cell site location data for an extended time period is unconstitutional. 161 The Court recognized cellphone users maintain reasonable privacy expectations in their historical cell site location data when it provides a detailed account about a person’s past movements. 162 The Fourth Circuit rejected the application of the third-party doctrine because cellphone users do not voluntarily convey their cell site location data. 163

The Third Circuit also noted that cellphone users do not voluntarily share their location information. 164 Rather than applying the third-party doctrine, the Third Circuit instead compared cell site location data to the beeper devices in United States v. Knotts 165 and United States v.


160. See Graham, 796 F.3d at 344-45. See generally United States v. Davis, 785 F.3d 498 (11th Cir. 2015); In re United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); In re United States for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t, 620 F.3d 304 (3d Cir. 2010).

161. See Graham, 796 F.3d at 361.

162. See id. at 349-59 (holding that there was a search when officers inspected defendant’s historical cell site location data up to 221 days). But see United States v. Davis, 785 F.3d 498, 516 (11th Cir. 2015) (holding that defendant had no privacy interest in a full comprehensive account of his past movements because the cell tower site did not create an “intimate portrait of [his] life”).

163. Graham, 796 F.3d at 354-55 (noting that cell site location data is automatically generated without any voluntary movement from a cellphone user).

164. United States for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t, 620 F.3d 304, 317 (3d Cir. 2010).

165. United States v. Knotts, 460 U.S. 276 (1983). Here, officers received consent from a company to install a tracking beeper inside a five-gallon container of chloroform. Id. at 278. The company’s former employee had purchase chemicals for drug manufacturing. Id. Unaware about the beeper, the former employee placed the container inside his car. Id. Officers used the beeper for visual surveillance up until the vehicle reached a private residence. Id. at 278-29. The Court held there was no search because a “person traveling in an automobile on a public thoroughfares has no
Karo. Ultimately, the Third Circuit held that was not a search because, unlike the beeper in Karo, the cell site location data did not reveal anything inside defendant’s private residence.

In contrast, the Eleventh and Fifth Circuits upheld the SCA’s reasonable suspicion standard for accessing cell site location data. Both circuit courts found the third-party doctrine applied because cellphone providers collect and store cell site location data as a business record. These circuit courts also noted that cellphone users assume the risk because they should know that cellphones must send signals to the nearest cell tower for their call to connect.

Indeed, these cases show that with four circuit courts applying different rationales for cell site location data, there is little guidance as to SCA’s proper standard. Ultimately, a warrant should be required

reasonable expectation of privacy in his movements from one place to another.” Id. at 281.

166. United States v. Karo, 468 U.S. 705 (1984). Similar to Knotts, after receiving consent, federal agents installed a beeper into a container of ether. Id. at 708. The beeper was used to track the container from a storage facility to several locations, including defendant’s private residence. Id. at 708-09. Unlike Knotts where agents monitored the defendant on a public highway, here, agents used the beeper to reveal information inside defendant’s residence. Id. at 714-15. The Court held that there was a search because agents without a warrant “obtain[ed] information that [they] could not have obtained by observation from outside the curtilage of the house.” Id. at 715.

167. In re The United States for an Order, 620 F.3d at 312.

168. Id. at 312-13.

169. See United States v. Davis, 745 F.3d 1205, 1217 (11th Cir. 2014) (holding that defendant did not voluntarily disclose his historical cell site location data, as to relinquish a reasonable expectation of privacy), reh'g en banc granted, opinion vacated, 573 F. App’x. 925 (11th Cir. 2014), rev’d en banc; 785 F.3d 498, 505-06 (11th Cir. 2015); In re United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

170. Davis, 785 F.3d at 511; In re United States for Historical Cell Site Data, 724 F.3d at 611-12.

171. Davis, 785 F.3d at 511-12; In re Application of the United States for Historical Cell Site Data, 724 F.3d at 612-13.

172. Compare United States v. Graham, 796 F.3d 332, 354 (4th Cir. 2015) (holding that a cellphone user does not voluntarily reveal his cell site location information because a service provider automatically generates such data in response to connections made between the cellphone and the providers network), and In re Application of the United States for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t, 620 F.3d 304, 317 (3d Cir 2010) (noting that
because cell site location data may track the movements inside an individual’s home; therefore, it intrudes on that individual’s reasonable expectation of privacy.\textsuperscript{173}

V. A NEW DIRECTION FOR FOURTH AMENDMENT JURISPRUDENCE

The United States Supreme Court has preferred to make bright-line rules for police officers.\textsuperscript{174} Yet, the SCA fails to provide simple guidance for officers because it mandates different procedures for various types of electronic information.\textsuperscript{175} Given that technology has evolved exponentially, the Court should modernize the third-party doctrine to afford emails and cell site location data Fourth Amendment protection; thus, requiring Congress to amend the SCA.

According to Professor Orin Kerr, Fourth Amendment jurisprudence is based on an equilibrium-adjustment in response to changes in technology and societal expectations.\textsuperscript{176} The purpose behind equilibrium-adjustment is to balance the needs between privacy interests and law enforcement.\textsuperscript{177} As technology progresses and

\begin{quote}
"when a cell phone user receives a call, he hasn’t ‘voluntarily exposed anything at all.’), with Davis, 785 F.3d at 512 n.12 (explaining that cellphone users voluntarily convey their cell site location data to their cellphone providers whenever they make or receive a call on their cellphone), and In re Application of the United States for Historical Cell Site Data, 724 F.3d at 613-14 (noting that cellphone users knowingly convey general location data to cellphone providers).
\end{quote}

\begin{quote}
174. Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981) (quoting Dunaway v. New York, 442 U.S. 200, 213 (1979) (White, J., concurring)) (noting that “if police are to have workable rules, the balancing of the competing interests inherent in the Terry principle, ‘must in large be part done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.’ The rule we adopt today does not depend upon such an hoc determination, because the officer is not required to evaluate either the quantum of proof justifying the detention or the extent of the intrusion to be imposed by the seizure.").
176. Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 HARV. L. REV. 476, 480 (2011) [hereinafter Kerr, Equilibrium] (describing equilibrium adjustment as a “correction mechanism” to Fourth Amendment jurisprudence because it is a judicial response from technological changes and social practice when technological tools and “new practices threaten to expand or contract police power in a significant way”).
177. See id. at 482.

Published by CWSL Scholarly Commons, 2016
threatens that balance, judicial interpretation from the United States Supreme Court restores the status quo.\(^\text{178}\)

However, there are judicial delays before there is an equilibrium-adjustment.\(^\text{179}\) The Court may risk erroneous adjustments because technology has yet to evolve to a stabilized state or societal practices related to the technology at hand continue to evolve.\(^\text{180}\) As an example, Professor Kerr points to the near forty-year gap in Katz’s reversal of Olmstead.\(^\text{181}\) To test the validity of equilibrium-adjustment, the next subsection will analyze United States Supreme Court decisions concerning surveillance technology.\(^\text{182}\)

\[\text{A. The Validity of Equilibrium-Adjustment}\]

Over the last thirty years, a perplexing issue for the Court has been applying the Fourth Amendment to surveillance technology.\(^\text{183}\) Most recently, in United States v. Jones\(^\text{184}\) and California v. Riley,\(^\text{185}\) the Court suggested that changes in technology might provide a new direction for Fourth Amendment jurisprudence.\(^\text{186}\)

In Jones, the Court held that attaching an electric monitoring device to a person’s vehicle without a warrant constituted a search.\(^\text{187}\) Some may argue that this holding tilted the balance towards more privacy rights because officers must secure a warrant before using a GPS tracker

\(^{178}\) Id. at 487-88.  
\(^{179}\) Id. at 539.  
\(^{180}\) Id.  
\(^{181}\) Id.  
\(^{182}\) Kerr’s article on equilibrium-adjustment was published in 2011. This was before the decisions in Jones and Riley.  
\(^{183}\) See, e.g., Kyllo v. United States, 533 U.S. 27, 34-35 (2001) (holding that the use of a thermal image outside a house to detect whether defendant was growing marijuana was a search because it was a technological tool inaccessible to the public); California v. Ciraolo, 476 U.S. 207 (1986) (holding that a plane flying at 1,000 feet in the air was not a search because the Fourth Amendment does not require officers to “shield their eyes when passing by a home on a public thoroughfare”); Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986) (holding that taking aerial photographs while flying at a navigable altitude was not a search).  
\(^{186}\) See id. at 2491-93; Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring).  
\(^{187}\) Jones, 132 S. Ct. at 949 (majority opinion).
device.\textsuperscript{188} Yet, this holding did not seem to shift the scale towards privacy interests because it has been long established that in appropriate circumstances, a warrant is preferable.\textsuperscript{189} The FBI agents in Jones secured a warrant; however, the agents exceeded the scope of the warrant.\textsuperscript{190} Rather than tilting the balance towards privacy interests, Jones left open the question whether a warrant is required when long-term surveillance might reveals one's daily activities.\textsuperscript{191}

Although the majority in Jones held that there was a search, the concurring opinions criticized the majority's reasoning for applying a physical trespass rationale.\textsuperscript{192} Both concurrences emphasized that the Court's rationale should have utilized a reasonable expectation of privacy test.\textsuperscript{193} The concurring opinions established that long-term monitoring violates reasonable expectations of privacy.\textsuperscript{194} As emphasized by the concurring opinions, the majority's decision presented "little guidance"\textsuperscript{195} and "vexing problems."\textsuperscript{196} Without this clear guidance, no adjustments were made because Fourth Amendment jurisprudence remained the same and individuals' privacy interests did not outweigh the needs of law enforcement.\textsuperscript{197}

On the other hand, Riley tilted the scale towards privacy interests.\textsuperscript{198} Riley involved two consolidated cases concerning whether police officers are authorized to search a cellphone as a search incident to arrest.\textsuperscript{199} In 1969, in Chime\textsuperscript{\textsuperscript{1}1\textsuperscript{\textsuperscript{v}} v. California,\textsuperscript{200} and in 1973, in United States v. Robinson,\textsuperscript{201} the Court held that officers could lawfully

\begin{itemize}
  \item \textsuperscript{188} See id. at 949.
  \item \textsuperscript{190} Jones, 132 S. Ct. at 948.
  \item \textsuperscript{191} See id. at 958 (Alito, J., concurring).
  \item \textsuperscript{192} See id. at 955 (Sotomayor, J., concurring); id. at 958 (Alito, J., concurring).
  \item \textsuperscript{193} See id. at 955 (Sotomayor, J., concurring); id. at 958 (Alito, J., concurring).
  \item \textsuperscript{194} Id. at 955 (Sotomayor, J., concurring); id. at 964 (Alito, J., concurring).
  \item \textsuperscript{195} Id. at 955 (Sotomayor, J., concurring).
  \item \textsuperscript{196} Id. at 962 (Alito, J., concurring).
  \item \textsuperscript{197} Cf. Kerr, Equilibrium, supra note 176, at 537.
  \item \textsuperscript{198} See Riley v. California, 134 S. Ct. 2473, 2484-85 (2014).
  \item \textsuperscript{199} Id. at 2480-81.
  \item \textsuperscript{200} Chimel v. United States, 395 U.S. 752 (1969).
  \item \textsuperscript{201} United States v. Robinson, 414 U.S. 218 (1973).
\end{itemize}
conduct a search incident to an arrest against an arrestee.\textsuperscript{202} By 2014, the Court refused to expand searches incident to an arrest to the digital data in cellphones.\textsuperscript{203} Notably, the Court recognized the implications of digital data searches in the twenty-first century.\textsuperscript{204} The Court determined that the privacy interest associated with the digital data in cellphones substantially outweigh the needs of law enforcement.\textsuperscript{205}

Applying the rationale in Chimel and Robinson, the Riley Court held that the digital data in cellphones, unlike physical objects, are less likely to pose harm against an officer.\textsuperscript{206} Cellphones are both qualitatively and quantitatively different compared to physical objects on an arrestee’s person.\textsuperscript{207} The Court emphasized that a cellphone’s massive storage capacity allows it to contain “the privacies of life” for many Americans.\textsuperscript{208} Therefore, the Court’s message was clear: officers need a warrant to search a cellphone.\textsuperscript{209} This holding adjusted Fourth

\textsuperscript{202} Id. at 235 (holding that searches incident to arrest are reasonable regardless of the “probability in a particular arrest situation that weapons or evidence would in fact be found.”); Chimel, 395 U.S. at 762-63 (holding that officers’ search of defendant’s entire house incident to arrest was unreasonable because the search must be within the area where an arrestee might have a weapon or destroy evidence); see also Thornton v. United States, 541 U.S. 615, 623-24 (2004) (extending searches incident to arrest inside the vehicle to include the entire passenger’s compartment when there is reason to believe evidence may be found even though defendant was in custody and there was no threat to officer safety). But see Arizona v. Gant, 556 U.S. 332, 343 (2009) (limiting Chimel and Belton in holding that searching the vehicle’s passenger compartment incident to arrest is only reasonable when “the arrestee is unsecured and within reaching distance of the passenger compartment”). In Gant, defendant was inside the squad car after officers arrested him for driving with a suspended license. Id. at 344. As a search incident to arrest, officers searched the inside of defendant’s vehicle. Id. The Court found it unlikely that there was evidence inside the passenger compartment because it was unrelated to defendant’s offense. Id.; see also Knowles v. Iowa, 525 U.S. 113, 118-19 (1998) (holding that a search incident to issuing a citation is unreasonable because the threat to an officer’s safety is less likely compared to a custodial arrest).

\textsuperscript{203} Riley, 134 S. Ct. at 2493.

\textsuperscript{204} See generally id. at 2489-95 (discussing the privacy implications that would occur if officers are allowed to conduct warrantless searches on cellphones).

\textsuperscript{205} See id. at 2493-94.

\textsuperscript{206} Id. at 2485.

\textsuperscript{207} Id. at 2488-89.

\textsuperscript{208} Id. at 2494-95 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

\textsuperscript{209} Id. at 2495.
Amendment precedent in line with technological changes.\textsuperscript{210} The question remains whether Riley tilted the scale towards privacy interest in a way that limits law enforcement’s needs to apprehend criminal activity and preserve officer safety.

It is unlikely that Riley’s holding put a burden on law enforcement’s needs to catch criminals and preserve officer safety. In Riley, the Court noted that officers are allowed to examine a cellphone’s physical aspect to eliminate any potential threat.\textsuperscript{211} It also found that there is unlikely any destruction of evidence once officers secure a cellphone.\textsuperscript{212} In fact, as technological advances increase, warrants are more readily accessible.\textsuperscript{213} Officers can request a warrant via email to a judge using an iPad, and receive a warrant within fifteen minutes.\textsuperscript{214} Therefore, it is fair to say that Riley’s holding did not implicate law enforcement’s needs to preserve evidence of criminal activity and to protect officer safety. While some may argue that Professor Kerr’s theory may seem conceptually too simplistic and broad, the Court’s rationale has indirectly applied Professor Kerr’s equilibrium adjustment theory when it has repeatedly balanced the competing governmental interest and individual interest at issue.\textsuperscript{215}

Despite Riley’s holding, there is still uncertainty whether electronic information stored to a service provider is afforded Fourth Amendment protection. The Court emphasized that the Riley decision did “not implicate the question whether the collection or inspection of

\textsuperscript{210} See Kerr, Equilibrium, supra note 176, at 487-88.
\textsuperscript{211} Riley, 134 S. Ct. at 2485.
\textsuperscript{212} Id. at 2486. The government, however, argued that there is a risk because cellphones are vulnerable to remote wiping and data encryptions. Id. Unconvinced, the Court noted that officers could take remedial measure to prevent remote wiping and data encryptions. Id. at 2487.
\textsuperscript{213} See id. at 2493 (citing Missouri v. McNeely, 133 S. Ct. 1552, 1561-63 (2013) (Roberts, C.J., concurring in part and dissenting in part)).
\textsuperscript{214} Id. at 2493 (quoting McNeely, 133 S. Ct. at 1561-63 (Roberts, C.J., concurring in part and dissenting in part)).
aggregated digital information amounts to a search under other circumstances." Nevertheless, the Riley and Jones rationales provide the best indication whether the Court would reconsider the third-party doctrine in the digital age world.

**B. The Privacy of Our Information**

Law enforcement’s authority to access emails has not been litigated as much in the criminal context, as compared to cell site location data. Nevertheless, SCA’s language as applied to emails is rampant with legal fallacies that should be rendered unconstitutional.

In *United States v. Warshak*, the Sixth Circuit ruled that the third-party doctrine was inapplicable to the contents of emails because the service provider was merely acting as an intermediary. Opponents may argue that emails are not entitled to Fourth Amendment protection under the third-party doctrine. Yet, Warshak’s rationale on the third-party doctrine is supported under Riley concerning warrantless searches of digital data on cellphones.

Many statements made in Riley about a cellphone’s notable features bolster the conclusion that emails are constitutionally protected. The Court described a cellphone as a “minicomputer[,]” emphasizing its immense storage capacity. While a standard cellphone contains sixteen gigabytes, a free email account with Google or Yahoo comes with at least fifteen gigabytes. Warrantless access to emails gives the government the ability to keep a watchful eye on people and learn about one’s particular daily activities. Like cellphones, an email has the

216. Riley, 134 S. Ct. at 2489 n.1; see also infra Section V.B-C.
218. Warshak v. United States, 631 F.3d 266 (6th Cir. 2010).
219. Id. at 288.
220. See Riley, 134 S. Ct. at 2489.
221. Id.
223. See Warshak, 631 F.3d at 284-85.
ability to store countless information on a web-based account that reveals the "privacies of life." 224

Most importantly, Riley seems to hint that the content on remote servers is protected. 225 Notably, the Court discussed special concerns that extending cellphones as a search incident to arrest may accidentally lead to searches on cloud-based data. 226 While the government attempted to justify a search of cellphones, the Court noted that searching cloud-base data is like "finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." 227 This is a strong analogy because common law long established that "every man's house is his castle," amounting to the greatest Fourth Amendment protection. 228 If a cellphone is a key, then the cloud-based data is presumably the castle. 229 Therefore, Warshak's decision along with Riley's reasoning about cellphones should be applied to emails for the Court to make necessary adjustments.

224. Cf. Riley, 134 S. Ct. at 2489. Many online services that are considered daily activities require an email account, including LinkedIn, Amazon, and Facebook. See AMAZON, http://www.amazon.com (last visited April 5, 2016); LINKEDIN, https://www.linkedin.com (last visited April 5, 2016); Facebook, https://www.facebook.com (last visited April 5, 2016).

225. See Riley, 134 S. Ct. at 2495.

226. See id. at 2491. A cloud-based data allows users to connect wirelessly and display data on a remote server. Id.; see also Quentin Hardy, The Era of Cloud Computing, NY Times (June 11, 2014, 7:57 PM), http://bits.blogs.nytimes.com/2014/06/11/the-era-of-cloud-computing/?_r-1 (discussing the impact cloud computing serves because it saves resources due to the amount of data users can stored and transfer among other networks).

227. Riley, 134 S. Ct. at 2491.

228. See, e.g., Payton v. New York, 445 U.S. 573, 596, 597 n.45 (1980) (quoting John Adams, in 2 LEGAL PAPERS OF JOHN ADAMS 142 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965)) (discussing that "one of the most essential branches of English liberty is the freedom of one's house. A man's house is his castle; and while he is quiet, he is as well as a prince in his castle."); Georgia v. Randolph, 547 U.S. 103, 115 (2006); Silverman v. United States, 365 U.S. 505, 511-12 n.4 (1961); see also Coolidge v. New Hampshire, 403 U.S. 443, 478 (1971) (holding that warrantless search on a man's castle is unreasonable unless there exists "a number of well-defined exigent circumstances").

C. The Privacy of Our Movements

Unlike emails, SCA's application to cell site location data has been hotly debated among federal appellate courts. While cell site location data reveals non-content information, it raises a constitutional concern because it creates an "intimate picture of [one's] life." The Court has also recognized that with further advances in surveillance technology, it might need to re-consider the decision whether long-term monitoring is unconstitutional. Given the practical necessity to use third parties in the digital world, a normative inquiry must be taken into account where individual subjective privacy expectations have been "condition[ed] by influences alien to well-recognized Fourth Amendment freedoms."

Yet, as Smith v. Maryland and United States v. Miller made clear, voluntarily conveying information to a third party relinquishes the warrant requirement. Nevertheless, the Fifth Circuit and Eleventh Circuit interpreted the third-party doctrine broadly and without

230. See supra Part IV.B.
231. See United State v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), aff'd sub nom, United States v. Jones, 132 S. Ct. 945 (2012). The D.C. Circuit Court described short-term surveillance on an individual's movements in separate isolated incidents as lawful; however, prolonged surveillance in the aggregate may violate reasonable expectations of privacy because it illustrates an "intimate picture of one's life." Id. This is known as the "mosaic theory," where "prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation." Id. This enables discovery about a person's "public movements that reflects a wealth of detail about [one's] familial, political, professional, religious, and sexual associations." Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring).
232. United States v. Knotts, 460 U.S. 276, 283-84 (1983) (noting that "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be a time enough then to determine whether different constitutional principles may be applicable.").
233. Jones, 132 S. Ct. at 957 (noting that the third-party doctrine is ill-suited in today's digital world because "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").
235. See Smith, 442 U.S. at 745-46; United States v. Miller, 425 U.S. 435, 443-44 (1976); see also supra Part II.B.
limitation, despite both circuits recognizing how technological innovation may change societal expectations of privacy.\textsuperscript{236}

The Fifth Circuit and Eleventh Circuit’s application of the third-party doctrine to cell site location data is wrong. The third-party doctrine is not supposed to eliminate Fourth Amendment protections when new technology provides alternative means to access information that previously required a warrant.\textsuperscript{237} Even Maryland’s former Attorney General Even Sachs, who argued \textit{Smith}, agrees that the \textit{Smith} case has been misinterpreted.\textsuperscript{238} \textit{Smith} is a different realm from today’s “massive intrusion” on American privacy.\textsuperscript{239} Unlike handing a bank deposit slip or dialing a numerical digit on a telephone, “cell site location data is not visible or tangible,” and cellphone users take no affirmative act to share their location data to a third party.\textsuperscript{240} Given the technological advances since 1979, comparing the pen register used in \textit{Smith} and the financial records in \textit{Miller} is like “saying a ride on a horseback is materially indistinguishable from a flight to the moon.”\textsuperscript{241}

\textbf{D. Modernizing the Third-Party Doctrine}

Ultimately, the SCA creates a constitutional danger because officers do not have the “time or expertise” to determine what is needed

\begin{thebibliography}{99}
\footnotesize
\item 236. \textit{In re United States for Historical Cell Site Data}, 724 F.3d 600, 610-11 (5th Cir. 2013); \textit{see United States v. Davis}, 785 F.3d 498, 512 (11th Cir. 2015).
\item 239. \textit{See id.}
\item 240. \textit{United States v. Graham}, 796 F.3d 332, 355-56 (4th Cir. 2015).
\item 241. \textit{Cf. Riley v. California}, 134 S. Ct. 2473, 2488 (2014). Even during the last six years cellphones have evolved exponentially; \textit{see United States v. Jones}, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring). The Fifth Circuit and Third Circuit cases involved cellphone technology from 2010. At the time, cell site location data was only generated whenever a cellphone user made or received a call; \textit{see In re United States}, 724 F.3d at 612-13. Cell site location data now automatically generates to the nearest cell tower periodically. Geolocation Hearing, \textit{supra} note 148, at 50 (written testimony of Prof. Blaze); \textit{see also} Jones, 132 S. Ct. at 963 (Alito, J., concurring) (noting that the modern smartphone is equipped with a GPS device that enables law enforcement officials to pinpoint the cellphone’s exact location).
\end{thebibliography}
to access specific types of electronic communication. Such constitutional rights would go unprotected against arbitrary and intrusive invasions. This goes against the Founders’ intent that prompted the ratification of the Fourth Amendment.

Riley and Jones offer a new path to modernize the third-party doctrine. A good example for the Court to follow is the Hawaii Supreme Court’s decision in *State v. Walton.* The Hawaii Supreme Court considered three factors regarding whether a person is entitled to reasonable privacy expectations under the third-party doctrine: (1) whether the information reveals “intimate details [about] a person’s life”; (2) whether the release of information to a third-party was necessary; and (3) whether the release of information to a third-party was without realistic alternative. In light of the digital age, these factors allow for a flexible third-party doctrine where electronic information is stored on equipment owned by a private service provider.

However, it is unclear when the Court will make necessary adjustments to the third-party doctrine. Professor Kerr indicated that there are judicial delays before there is an equilibrium-adjustment. There was the forty year gap between *Katz* and *Olmstead,* and there was the forty-one year gap between *Robinson* and *Riley.* It has now been almost forty years since the decision in *Smith v. Maryland.* The Court has stated that it must preserve privacy protections that correspond with technological changes. Yet, the Court has also recognized that it must proceed with caution when considering privacy expectations and Fourth Amendment rights.

---

242. See Dunaway v. New York, 442 U.S. 200, 211-14 (1979); see also Oliver v. United States, 466 U.S. 170, 181-82 (1984) (noting that “this Court repeatedly has acknowledged the difficulties created for courts, police, and citizens by an ad hoc analysis, case-by-case definition of the Fourth Amendment standards to be applied in differing factual circumstances.”).

243. Oliver, 446 U.S. at 181-82.

244. See LASSON, supra note 27, at 54.


246. Id. at 907 (quoting Smith v. Maryland, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting)).

247. See id. at 906-07.


249. Id.; see also supra text accompanying notes 202-03.

Amendment issues related to emerging technology.\textsuperscript{251} Without judicial adjustments, Professor Kerr indicates that judicial delay would likely prompt legislative action.\textsuperscript{252}

VI. THE PROPOSED REVISION FOR THE STORED COMMUNICATIONS ACT

United States Supreme Court Associate Justice Samuel Alito has noted that Congress is in a better position to solve issues associated with electronic surveillance, rather than federal courts applying the Fourth Amendment.\textsuperscript{253} “A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy in a comprehensive way.”\textsuperscript{254} Congress or state legislatures should “enact legislation that draws reasonable distinctions based on . . . electronic surveillance.”\textsuperscript{255} Justice Alito’s message helped spark the enactment of California Senate Bill 178.\textsuperscript{256}

\textit{A. California Electronic Communication Privacy Act of 2016}

California recently enacted Senate Bill 178, reaffirming the requirements for law enforcement to obtain electronic stored information.\textsuperscript{257} Senate Bill 178, known as California Electronic Communication Privacy Act (“CalECPA”) of 2016, went into effect January 1, 2016.\textsuperscript{258} CalECPA requires officers to secure a warrant based

\begin{itemize}
\item[251.] City of Ontario, Cal. v. Quon, 560 U.S. 746, 759 (2010).
\item[252.] See Kerr, \textit{Equilibrium}, supra note 176, at 541.
\item[254.] Jones, 132 S. Ct. at 964 (Alito, J. concurring).
\item[255.] Riley, 134 S. Ct. at 2497 (Alito, J., concurring).
\item[258.] Patrick McGreevy et al., \textit{California’s New Laws for 2016: See How You Are Affected}, LOS ANGELES TIMES (Dec. 31, 2015, 12:05 AM),
\end{itemize}
A NEW AGE LOOK AT OLD SCHOOL PRIVACY LAWS

upon probable cause before accessing any electronic stored information.  
Electronic stored information includes content information like emails, digital documents, and digital data stored on the cloud while non-content information includes any metadata information like cell site location data. Accordingly, CalECPA expands and strengthens privacy legislation that corresponds with modern technology. Amending the SCA similar to CalECPA would provide a uniform, standardized bright-line rule for law enforcement. Therefore, Congressional efforts should follow California's lead.

B. Requiring a Search Warrant Creates Proper Transparency

Thirty years after the SCA’s enactment, it is apparent that the SCA is inadequate. With recent technological innovations, law enforcement agencies exploit outdated federal privacy legislation in accessing emails and using cellphones as tracking devices without a warrant. Following CalECPA would replace the distinctions between an ECS and an RCS, and would also provide a remedy provision similar to the exclusionary rule. Even the San Diego Police Officers Association supports CalECPA’s enactment because it “strengthens community


260. See MAINTENANCE OF THE CODES, ch. 86, sec. 233, § 1546.1. Section 1546(d) includes “sender, recipients, format, or location of the sender, or recipients at any point during the communication, the time or date of the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address.” Id.


262. Id. at 6-7.

263. CAL. PENAL CODE § 1546.4 (West 2016).
relationships and increases transparency [and] in the best interest of all Californians."²⁶⁴

Figure 1: This chart summarizes the different procedures to access electronic stored information under the SCA. Following CalECPA’s example will create privacy protections and create proper transparency and oversight among law enforcement agencies.

<table>
<thead>
<tr>
<th>SCA</th>
<th>Unopened email in electronic storage 180 days or less</th>
<th>Search Warrant required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCA</td>
<td>Unopened email in electronic storage more than 180 days</td>
<td>Subpoena with notice; 2703(d) court order; or search warrant</td>
</tr>
<tr>
<td>SCA</td>
<td>Opened email, remote computer service information</td>
<td>Subpoena with notice; 2703(d) court order; or search warrant</td>
</tr>
<tr>
<td>SCA</td>
<td>Non-content records</td>
<td>2703(d) court order or search warrant</td>
</tr>
<tr>
<td>SCA</td>
<td>Basic subscriber information: non-content information</td>
<td>Subpoena or 2703(d) court order.</td>
</tr>
<tr>
<td>CalECPA</td>
<td>Electronic Communication Information from a service provider</td>
<td>Warrant accompanying order requiring the service provider authenticate provided electronic information.</td>
</tr>
</tbody>
</table>

Opponents, however, may argue that this will overburden law enforcement. There is no denying that officers should have access to technological tools to aid their search for the truth.²⁶⁵ The societal interest in law enforcement using technological resources is important because it enhances criminal investigations to apprehend criminals.²⁶⁶ But, as like technology aids in criminal investigations, the exploitation of technological advances can also implicate the Fourth Amendment.²⁶⁷

²⁶⁵. United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015).
²⁶⁶. Id.
Accordingly, a warrant requirement to access emails and cell site location data should not be viewed as a burden on law enforcement. Instead, it should be viewed as proper transparency and a constitutional guide for law enforcement. The warrant requirement is a highly valued practice in the Constitution. Therefore, during routine criminal investigations, officers should seek a warrant to access electronic stored information site location data and emails, unless exigent circumstances arise.

CONCLUSION

Going back to the Paris attacks, increasing government surveillance is unnecessary. The United States already has the ability to monitor any individual. By focusing more on national security and limiting Fourth Amendment safeguards, statutory protections will continue to fail in providing a proper balance between privacy and public safety.

Instead, the question is how privacy legislation should change. What should privacy legislation protect, and to what extent? The SCA’s complex language and application is incompatible with modern technology. This Comment drew upon emails and cell site location data to show how the SCA consists of legal fallacies that implicate the Fourth Amendment.

Given that the SCA was enacted thirty years ago, this Comment also drew upon an alternative solution using Professor Kerr’s equilibrium-adjustment theory on Fourth Amendment jurisprudence. Whether the Court or Congress will act first is a matter of time. If the judiciary is to act first, it must recognize that evolving technology demands evolving law. Strictly applying Smith v. Maryland and United States v. Miller can no longer justify its broad application to any information conveyed to a third party. Doing so will ignore the impact electronic communication has on modern society.

On the other hand, Congress may be in a better position, as Justice Alito noted. If so, Congress should follow CalECPA’s example to provide a clear standard. Currently, the government’s ability to access

269. See id.
270. Id.
271. See McCarthy, supra note 11.
emails and cell site location data without a warrant violates people's personal freedom. This should not be allowed without a warrant or unless exigent circumstances arise.

Carlos Aguilar*

* * *  

California Western School of Law, J.D. candidate, 2017. San Diego State University, B.S. Criminal Justice, 2014. I would like to thank everyone on the California Western Law Review editing staff, in particular Jake Novack and Paige Woodward, for their tireless efforts in preparing this Comment for publication. Thank you to Professor Thyfault, Professor Yeager, and Will Hopkins for their guidance in the development of this Student Comment. Above all, I would like to dedicate this note to my family—I would not be the person I am today without their unwavering love and support.
INFORMATION FOR AUTHORs

The California Western Law Review welcomes the submission of unsolicited manuscripts concerning topics of legal interest. The Law Review prefers that all articles (and expedite requests) be submitted via ExpressO at http://law.bepress.com/expresso/. If you are unable to submit your article via ExpressO, please direct your submission via email to lawreview@cwsl.edu.

Please observe the following requirements for your submission:

(1) All citations should conform to The Bluebook: A Uniform System of Citation (20th ed. 2015).

(2) Manuscripts should be submitted in Microsoft Word format.

(3) Each manuscript should be accompanied by a cover letter giving a brief overview of the manuscript and providing author contact information including name, e-mail address, phone number, and mailing address. Enclosing a résumé, a list of previous publications, and/or a vita with the submission, while not necessary, can also be helpful for the Law Review’s reviewers.

Manuscripts will be approved for publication in the Law Review only after a Lead Articles Board review. If any part of the paper has been published elsewhere, the author must include this information at the time of submission. Submitted manuscripts will not be returned unless requested.

The California Western Law Review will do everything possible to ensure prompt review of submitted manuscripts. Please note that manuscripts which adhere to the above listed format will move through the review process more rapidly.
AN INVITATION TO EMPLOYERS
FROM
CALIFORNIA WESTERN SCHOOL OF LAW

California Western School of Law provides career services for students and recent graduates.

If your firm, agency, or organization is interested in interviewing individuals for associate positions, you may contact the Career Services office to make arrangements.

Please direct inquiries to:

Courtney Miklusak
Assistant Dean for Career and Professional Development Office

California Western School of Law
225 Cedar Street
San Diego, California 92101
Phone: (619) 525-1557
crm@cwsl.edu
www.cwsl.edu