Short-Circulating Legal Guidance in the Digital Age: An Evaluation of Inadequate Protections for the First and Fourth Amendments, and the Electronic Communication Privacy Act

Audrey Lorene Leeder

Follow this and additional works at: https://scholar.smu.edu/scitech

Recommended Citation
https://scholar.smu.edu/scitech/vol18/iss3/7

This Comment is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
Short-Circuiting Legal Guidance in the Digital Age: An Evaluation of Inadequate Protections for the First and Fourth Amendments, and the Electronic Communication Privacy Act

Audrey Lorene Leeder*

I. A CRIPPLING EFFECT OCCURS WHEN LAWS THAT GOVERN ADVANCE TECHNOLOGICAL CELLULAR PHONE SURVEILLANCE ARE INSUFFICIENT

"The first rule of any technology . . . is that automation applied to an efficient operation will magnify the efficiency. The second [rule] is that automation applied to an inefficient operation will magnify the inefficiency."¹ This quote from Bill Gates, founder of Microsoft Corporation, summarizes not only a very important principle about how technology is made, but also how society’s laws can affect how technology is used within the sphere of law. The United States’ advancement of, and reliance on, technology has revealed the inefficiencies of the laws that govern its use.

The U.S. Constitution was enacted to ensure that freedoms essential to fostering a successful democratic society were protected. For over 200 years, the Constitution has persevered through the issues facing the American public. History has shown that one of the main strengths of the Constitution is its constant and unfolding nature. This stability has provided a strong foundation to rely on during our nation’s weakest times, though some critics argue that this “constant and consistent” nature can be construed as rigid and inflexible. However, this critique ignores the fact that the Constitution was created in a time when America faced issues that are drastically different from the ones it faces today.

The American way of life has changed dramatically in the last 200 years due in large part to technological advancements. For example, things that did not exist when the Constitution was written are now viewed as essential parts of a habitable home; such items include light bulbs, electric stoves, air conditioning, and, importantly, cell phones. In this respect, the Constitution has encountered difficulties when adapting to this new view of life. This difficulty is particularly evident when applying Constitutional principles to cellular technology. Cellular phones have become a necessary aspect of American living. In fact, the federal government recognized the necessity of cellular

* Audrey L. Leeder is a 2016 candidate for Juris Doctor from SMU Dedman School of Law in Dallas, Texas. She would like to thank her loving family and friends who continually support and inspire her in life and legal career.

phones when it enacted the Lifeline Program; a plan that provides discounted cellular phones to impoverished citizens. Since cellular phones have become an essential part of communication, there must be laws that control the Government’s surveillance of their private use. Establishing new laws are necessary to guarantee the protection of users’ constitutional rights.

Currently, the federal government is relatively uninhibited in its surveillance capabilities with regard to cellular phones. As a result, the federal government freely utilizes this power to perform intimate searches of an individual’s personal life. This invasion directly infringes upon the First and Fourth Amendment, as well as statutory protections. As a remedy to these invasions, this comment urges the need for a new statute regarding cell phone privacy that better protects citizens’ First and Fourth Amendment rights. This statute must be more direct and effective than the current “solution” that the legislature has enacted; the Electronic Communications Privacy Act is insufficient to address these concerns. A failure to do so threatens the vitality of First and Fourth Amendment rights by destroying the American public’s security and trust in cellular phones.

The First and Fourth Amendments provide the most privacy protections to cell phone users. The First Amendment cultivates and encourages the exchange of ideas by affording specific protections to one’s speech and expression. It embraces an individual’s right to speak freely without having to worry about negative repercussions, and encourages an individual to associate with whomever he may choose. The Fourth Amendment also seeks to prevent unjustified intrusions and overly invasive investigations by the Government. Unfortunately, and contrary to the Founding Fathers’ intentions, these constitutional protections are consistently infringed upon by the Government.

While the establishment of the First and Fourth Amendments eased the Founders’ concerns, these amendments have also led to oversights and vulnerabilities in the legal system by creating a false sense of security. However, these constitutional protections do a disservice to the Founding Fathers’ ideas of protection of U.S. citizens. Our Founding Fathers envisioned a society where citizens were free to exchange ideas freely and without fear of reprisal, but because of the quick pace of the technological evolution in the United States, our laws have not been able to adequately protect these rights.

Technological advancements provide an important service to our developing society. For example, the use of technology alleviated the limited communication issue that plagued the American public. Things such as the Internet and cell phones created instant communication, and along with it provided a means for the Government to invade the lives of the American public like never before. One of the main culprits of producing such vulnerabilities is tracking technology, which increased the Government’s ability to efficiently to collect an individual’s cellular phone information. For instance,

global positioning systems (GPS) and subscriber identification module (SIM) cards track an individual’s location and store data information. Advanced cellular phones, such as those with iPhone or Android platforms, have GPS built into the phone to assist with locating your position and providing directions. This albeit convenient addition enhances the Government’s ability to closely monitor an individual’s movements.

While GPS is commonly implemented in only advanced phones, older phone users are not safe from the Government’s invasive cellular phone monitoring either. SIM cards are in nearly every phone in order to process data. A SIM card provides a way to track an individual carrying any cellular phone just as those that contain GPS. Because of these technologies, most cellular phones are quite capable of tracking an individual’s location through technology that is already within the device and that has historically been used to monitor individuals. Yet, Congress has not paid attention to the Government’s use of this technology to surveil its citizens or to the constitutional violations that might occur from such use.

A survey conducted for the purposes of this comment, which asked whether the respondent would alter their choice of association if they knew the Government had the ability to track their activities, revealed eye-opening results. Nearly forty-percent of those surveyed stated that they would not have behaved in the same manner had they known that the Government possessed the ability to track and search an innocent individual’s cellular phone. Several of the respondents who stated that they would not alter their activity believed that the Government was already tracking their activity. Based on their responses, the overall number of individuals directly affected by the Government’s domestic surveillance through cellular phones is more than forty-percent.

Additionally, the study revealed that nearly fifty-percent of respondents between the ages of twenty-one and forty, expressed that they would not alter their behavior. Given the pervasiveness of the technology in young adults it is likely that the more engrained the use of a cellular phone is in an individual’s life, the more he or she will trust the device and provider. This in turn decreases the likelihood that the individual will believe the Government can track his or her personal device. Accordingly, rising generations will be less suspicious of the Government, less likely to question its motives, less likely to protect themselves against invalid methods of surveillance, and more vulnerable to infringement. It is these precise individuals, who do not contemplate protecting themselves from the Government, that are in the most need of adequate statutory protections. The survey findings also illustrate a statutory gap; the individuals who need the most protection do not seek it. This mentality underlines a crucial vulnerability faced by the American public. Without statutes that directly address the issue of cellular phone surveillance, individuals will continue to disregard their constitutionally-protected right to

3. See infra Appendix A. The Survey polled thirty-one individuals between the ages of twenty-one and seventy-seven.
both associate without government intrusion, and to prevent unjustified meddling into their private lives.

A cellular phone has the potential to hold more private and intimate information than any other single item seized from a governmental search. An intimate text message conversation between two individuals could fill multiple diaries, day planners, or portfolio pages. Cellular phones are susceptible to unconstitutional government surveillance. Currently, there is no adequate law in place to monitor and limit the Government's ability to take advantage of the vulnerabilities our society has created through our reliance on technology. A potential solution to this issue is to incorporate the policies that underlie First and Fourth Amendment protections through legislation. Attention to First Amendment values would alleviate privacy concerns produced by cellular phone surveillance by limiting the Government's ability to track and search to only those instances where an individual's constitutionally protected rights to free speech, expression, and association are not infringed. Additionally, the spirit of the Fourth Amendment would limit governmental invasions through a search and seizure analysis that applies to the tracking of cellular location. These limitations would also reduce the chilling of speech, an apparent fear, evidenced by the survey referenced above.

A. Roadmap to the First and Fourth Amendments' Infringement of Cellular Phone Tracking and Data Invasion

This comment seeks to shed light on the invasion of cellular phone tracking that has crept up on the American public. First, this comment will address the historical background of the U.S. government's use of surveillance. Generally, the history of the United States illustrates areas of weakness from which the Government can learn from to prevent failing at similar issues in the future. Second, this comment will draw on the uniquely analogous issue of wiretapping surveillance for guidance in the proper procedures to control cellular surveillance. The United States faced a similar issue to the current cellular surveillance when it dealt with wiretap surveillance only fifty-years earlier. Third, the Government's current use of tracking an individual's cellular phone location and its implications will be analyzed. Fourth, this comment will discuss the current laws prohibiting the Government's ability to track cellular phones and search cellular phone data. Finally, a statutory solution will be proposed to protect the future of America in the digital age. Each section will be divided into subsections to further analyze the details of each area. These sections will highlight the natural extension and necessary implementation of the First and Fourth Amendments in a new statute. The First and Fourth Amendments, federal statutes, and judicial precedent will provide the foundation for a functional, efficient, and necessary statutory enactment to protect the American public from a digital age invasion.
II. THE HISTORY OF THE FEDERAL GOVERNMENT’S USE OF SURVEILLANCE

Historically, the Constitution was adapted in an attempt to restrict the federal government’s ability to invade an individual’s personal information. Although the federal government uses its surveillance powers to legitimate ends, such as the executive branch’s use of citizen surveillance, cellular phones have increased the Government’s ability to surveil by creating a more accessible method of collection. The accessibility of data on a person’s cellphone is problematic because it has become an efficient means to distribute this private information to third parties.

The modern American citizen is likely screened by the Government on a daily basis. Surveillance techniques permeate the average American’s life—benign trips to the supermarket are captured by security cameras; every call and text from a cellular phone is recorded and processed. The federal government can easily acquire a citizen’s communication information through cellular phone call records, as well as GPS and SIM card tracking. This section will address the issue of increased surveillance over the past 200 years. American surveillance can be separated into two distinct eras: (1) the era of government limitation and suppression; and (2) the era of acceptance of government surveillance.

A. The Era of Government Limitation and Suppression of Surveillance

Prior to the 20th century, the Government’s surveillance of the public was limited to national security purposes during times of war. For instance, during the Revolutionary War, the Committee for Detecting and Defeating Conspiracies gathered information from suspected British spies and supporters. Additionally, during the Continental Congress, members stole and read mail addressed to the Tories. Finally, the Sons of Liberty advanced surveillance techniques by collecting information for the revolutionists. Common to all of these methods of surveillance in the early years of America was the

6. Solove, supra note 4, at 114.
8. Id.
9. Id.
10. Id.
element of aiding in war efforts, and not a mere a desire to investigate citizen's personal lives.

B. Pre-1900

While the United States had obtained several intelligence-gathering streams within the first few years of independence, the end of the Revolutionary War and the enactment of the Constitution stalled this progression. In 1865, Secretary of State William Seward attempted to counteract this stagnation by creating a surveillance network known as the Secret Service. The Secret Service was created as a clandestine network, operating across the United States and Canada. Shortly before the end of the Civil War, the Confederacy also established a surveillance network, the Secret Service Bureau, but its activities, shrouded in secrecy, vanished over time. As with the end of the Revolutionary War, the end of the Civil War also experienced a lull in surveillance advancements, despite the previous creation of the Secret Service and Secret Service Bureau. This pattern of stagnation enforces the idea the aim of surveillance pre-1900s was used almost exclusively during times of hostility and war.

C. Post-1900

The Red Scare further justified the use of surveillance to proactively protect national security and quickly reestablished surveillance methods as a priority. Since this time, for better or worse, Americans have lived with constant surveillance. The decision to increase domestic surveillance created a deep rift between the judicial and legislative branches, and the executive branch. The executive branch sought to expand its powers through an

11. Id.
12. Id. at 107–73.
13. Donahue, supra note 7, at 1073.
14. Id.
15. Id.
17. Donahue, supra note 7, at 1073.
18. See generally id. (detailing the history of surveillance in the United States).
19. Id. at 1073.
increase in domestic surveillance, while Congress and the judiciary acted affirmatively to limit this expansion.20

However, after a decade of severe violence post-World War I, all three branches of the federal government united to increase domestic surveillance in an effort to ease the fighting.21 Attorney General A. Mitchell Palmer and J. Edgar Hoover, the future director of the Federal Bureau of Investigation (FBI), led this new drive for surveillance.22 Beginning in 1919 the federal government, led by Palmer and Hoover, also intensified its surveillance efforts.23 These efforts appeared to pay off when in a single day, and across 33 cities, the Government located and deported more than 4,000 undesirable aliens who were believed to be communists.24 However, it was later revealed that the raid was barely a drop in the bucket as more than 26,000 American communists existed at that time.25

Technological advancements during the mid-1900s greatly enhanced the Government’s ability to monitor the public.26 Wiretaps were a monumental advancement in surveillance.27 The inception of the telephone brought with it the easily accessible and useful surveillance method of wiretapping a phone to eavesdrop on its users.28 Years after wiretapping was put into use the battle between privacy and national security went public as a result of the United States’ public acknowledgment of the Government’s use of clandestine tracking.29

The executive branch was concerned with expanding its own powers and continued to question the legislature’s alternative motives. President Truman worried about these potential alternative motives, established the National Security Agency (NSA) to oversee domestic surveillance.30 The Government used wiretaps throughout the Cold War to monitor conversations in hopes of tracking Soviet membership.31 Wiretaps became a central component of national and foreign surveillance.32 The NSA is now a massive

20. Id. “Congress barred the Department of Justice (DOJ) from employing Secret Service in an intelligence-gathering function.”
21. Id. at 107–74.
22. Id.
23. See Donahue, supra note 7, at 1073–74.
24. Id.
25. Id. at 1074.
26. Id. at 1070.
27. Id.
28. Id.
29. Donahue, supra note 7, at 1076.
30. Id. at 1080.
31. Id. at 1061, 1080.
32. Id. at 1072.
infrastructure that consumes a large share of the estimated $40 billion dollars budgeted annually for U.S. intelligence.33

The U.S. Supreme Court later limited the invasion of wiretaps into Americans’ lives by requiring warrants for domestic intelligence surveillance.34 In United States v. United States District Court, the Court stated: “the price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of government action in private conversation.”35 In this case, the Supreme Court recognized the First Amendment implications of monitoring Americans’ domestic activities by directly referencing concerns of chilling “vigorous citizen dissent and discussion of government action.”36

However, it became apparent that the NSA did not plan on adhering to this holding when it continued to conduct illegal domestic spying.37 The NSA surveillance monitored millions of domestic and foreign telegrams.38 As a response to the NSA’s defiance of judicial precedent, Congress created the “Church Committee,” which recommended legislative reform on domestic surveillance.39 The Church Committee analyzed and compiled reports regarding the federal government’s domestic surveillance procedures.40 The Church Committee “reported that there was ‘frequent testimony that the law, and the Constitution were simply ignored’ and that there was a ‘general attitude that intelligence needs were responsive to a higher law,’ namely, ‘national security.’”41

The Church Committee alleged in their reports that government surveillance conducted in the name of national security was a ruse used to cover the actual reason for the surveillance—political control.42 For example, President Johnson at one point requested information regarding individuals’ political associations.43 The Church Committee’s findings stated that in fact a sub-

33. Bloom & Dunn, supra note 5, at 153.
35. Id. at 314.
36. Id.
38. Id. at 30.
39. Id.
40. Id.
41. Id.
42. Id.
43. Dranias, supra note 37, at 30.
stantial portion of the surveillance for the purposes of obtaining political information; national security concerns were just an added benefit.44

Due to the startling revelations regarding the Government’s deception, the Church Committee felt it necessary to make a serious change. In an attempt to make such a monumental change, its final report recommended that Congress take action to enact a “clearly defined and effectively controlled domestic intelligence capability, which included the establishment of various legal barriers between foreign and domestic intelligence agencies.”45 “[T]he unifying principle underlying [the Church Committee’s] recommendations was the recognition of the ‘fundamental’ need to protect American citizens from intelligence gathering based predominantly on their domestic First Amendment activities.”46 Unfortunately, there was little action taken on the Church Committee’s recommendations,47 and the Government was essentially returned to the pre-committee state.

Because the Church Committee had little effect, in 1978 the Senate once again acknowledged the need to limit government surveillance by enacting the Foreign Intelligence Surveillance Act (FISA).48 Particularly, FISA reiterated the Supreme Court’s requirement from United States v. United States District Court requiring government entities to acquire a warrant before eavesdropping on private conversations.49 FISA remained the central entity that limited the Government’s surveillance methods until the twenty-first century and still retains a considerable amount of control. Up until 2001, both the judiciary and legislature feared the Government’s surveillance techniques because they were thought of as an over-expansion of the executive branch’s powers as well as an invasion of private matters.50 This fear persisted until our nation’s worries were set on directed to international enemies, reviving the expansion of domestic surveillance.

D. The Era of the Public’s Acceptance of Government Surveillance

September 11, 2001, a day that will forever be engrained in the soul of America, changed citizens’ views of surveillance and set an unprecedented acceptance of surveillance techniques. The terrorist attacks on September 11 created a culture shift; Americans began to appreciate, accept, and even desire domestic surveillance. The rift that existed between the branches of the federal government seemed to vanish after the attacks.51 One of the worst

44. Id.
45. Id. (internal citation omitted).
46. Id.
47. See Donohue, supra note 7, at 1092.
48. Id. at 1094.
49. Id.
50. Id. at 1073.
51. Id. at 1101.
moments in American history, a moment that ripped hope from millions of American’s hearts, also opened their eyes and locked their sights on preventing terrorism. This hatred set forth an anti-terrorism program centered on both domestic and foreign surveillance.52

Riding this wave of patriotism, President Bush established the NSA Domestic Spying Program, which allowed the Government to eavesdrop on domestic phone calls.53 Subsequently, in late 2002, telecommunication companies, including AT&T, BellSouth, and Verizon, voluntarily entered into agreements with the NSA, releasing mass quantities of their customers’ cellular phone usage information to the Government, in the name of national security.54 This voluntary disclosure is authorized by statute: a provider may release consumer information to the Government if the provider believes the Government requires the information for an emergency involving the danger of death, or serious injury to a person.55 However, these customers were never informed of the provider’s ability to, in good or bad faith, grant the Government access to their private information. Indeed, like any boilerplate contractual agreement, the number of consumers who actually understood that their contract with their cell phone provider condoned government eavesdropping is low.

Governmental eavesdropping on domestic and foreign conversations continued until October 2011, when a FISA court found part of the NSA’s surveillance program unconstitutional.56 Subsequently, the Government admitted to the unconstitutionality of some of the monitoring procedures, while defending and continuing to use others.57 Although the court did not find that the collection of the public’s data was unconstitutional, in dicta, the court criticized and expressed that it did not condone this technique.58 Thus, without further limitations, the collection of calling records persists today.59 Still, it is reasonable to infer from the court’s decision that the court would condone a law limiting the collection of data.

Over the last decade, Americans have come to expect surveillance of daily conversations and “Big Brother’s” constant, watchful eye on their private activities. For instance, while facial recognition cameras once existed only in science-fiction movies, they are now an essential part of major metropolitan surveillance. This acceptance of technological invasion has laid a

53. Id. at 878, 882.
54. Id. at 882.
56. See Sinha, supra note 52, at 897–98.
57. See id. at 927, 935–36.
58. Id. at 898.
59. See id. at 898–99.
foundation for further intrusion into an individual's life via cellular phone tracking and data invasion.

Though the landscape of surveillance has drastically changed in the last fifty years, the laws remain fairly the same. A once accepted method of protection has evolved into a different monster. To protect our society's closely held belief in privacy and free expression, the inadequacies of the First and Fourth Amendment, current statutory law, and judicial precedent must be addressed. Congress must seriously consider enacting new statutes to reform these issues.

III. THE ANALOGOUS ISSUE OF WIRETAPPING SURVEILLANCE IN RELATION TO CELLULAR PHONE SURVEILLANCE

The First and Fourth Amendments issues encountered with wiretapping are analogous to the issue of cellular phone surveillance. Wiretapping is a form of domestic surveillance that is relied on by the federal government with little thought as to the effect it has on the American public. The executive branch used wiretaps as an essential surveillance technique with few limitations until the judiciary and legislature attempted to implement regulations and statutes.\textsuperscript{60} However, these attempts by Congress and the Supreme Court to control the executive were mostly ignored.\textsuperscript{61} Eventually, Congress and the Court were able to reign over the executive by placing successful limitations on wiretaps.\textsuperscript{62} The history of wiretapping provides an example of the proper steps that the Government should take to implement cellular phone tracking without infringing on citizens' First and Fourth Amendment rights.

Warrantless wiretapping began in 1931 when the FBI used wiretapping to preserve national security.\textsuperscript{63} Wiretapping is a surveillance method that taps into a telephone wire when two individuals are speaking and transmits the conversation to a third party, enabling the that party to eavesdrop on the conversation. The use of wiretapping was commonly unopposed for foreign surveillance, but when it began to be used to spy on American citizens in the mid-nineteenth century, it was not as easily accepted.\textsuperscript{64} The likely cause of the adverse treatment of domestic wiretapping is that wiretapping implicates First and Fourth Amendment concerns regarding invasion of privacy and chilling of free speech.

\textsuperscript{60} Donohue, \textit{supra} note 7, at 1067.
\textsuperscript{61} See \textit{id.} at 1068.
\textsuperscript{62} See \textit{id.} at 1069.
\textsuperscript{63} Sinha, \textit{supra} note 52, at 869.
\textsuperscript{64} See \textit{id.} at 873.
The Supreme Court first ruled on the issue of wiretapping in 1928 in *Olmstead v. United States*. In *Olmstead*, the defendant was charged with liquor-related crimes during Prohibition. Specifically, he was charged with leading a liquor distribution ring. The liquor distribution ring included several stores across the United States and Canada. Due to the distance between these stores, the defendant was forced to conduct a majority of his business over the telephone. The federal government tapped into the defendant's telephone conversations and subsequently obtained information that directly led to his conviction. The defendant claimed a violation of his Fourth Amendment right to privacy. The Court held that the Government did not violate the Fourth Amendment, and that the wiretap was a permissive invasion because the Fourth Amendment is only implicated when the Government physically invades a citizen's tangible property. The *Olmstead* precedent practically eliminated a constitutional claim for illegal electronic communication surveillance.

The *Olmstead* ruling created an era where the federal government performed a slew of invasive wiretaps. For instance, during the 1930s, J. Edgar Hoover pushed for secret wiretapping missions in response to the national crisis posed by Russia. Invasive wiretapping continued into the 1940s and 1950s when Judith Coplon, a suspected Soviet, was arrested partially because of evidence that was obtained through an illegal wiretap. Although the Court took a stand against illegal wiretaps, the FBI continued to perform them.

In the 1960s, the laws regarding wiretapping were as undeveloped as today's area of law concerning cellular phone surveillance. In the 1960s, the Government utilized wiretaps for domestic surveillance of U.S. citizens. In addition, great tension existed between the federal branches regarding the proper usage of wiretaps. To unify the branches, President Johnson published a memorandum in 1965 banning the use of wiretaps, except for national security purposes. This decision was momentous because by this time it was

67. *Id.* at 455–56.
68. *Id.* at 456.
69. *Id.* at 456–57.
70. *Id.* at 456.
71. *Id.* at 455.
72. *Olmstead*, 277 U.S. at 466.
73. Donohue, *supra* note 7, at 1075.
74. *Id.* at 1076.
75. *Id.*
76. *Id.* at 1070.
77. *Id.* at 1077 n.83.
common for Americans to use landline telephones, and as a result this decision greatly restricted the most successful method of surveillance.

In 1967, the Court reevaluated its stance on electronic surveillance, overruling its holding in *Olmstead.* In *Katz v. United States*, the defendant used a public pay phone in Los Angeles to place wagers in Boston and Miami, a direct violation of federal law. The federal government had previously placed a recording device on the telephone booth to record the defendant’s illegal gambling. The Government acquired enough evidence through surveillance to convict the defendant of illegal gambling.

The Court held that “what [an individual] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” The Court replaced the interpretation of trespass under the Fourth Amendment by defining it as a “breach of an individual’s reasonable expectation of privacy.” Under this analysis, it is not the location of the action that the Court evaluates, but instead whether the individual’s actions were intended to be publicly or private.

In its majority opinion, Justice Stewart expressed that the Fourth Amendment applies in situations where the individual expects to have privacy, regardless of whether the physical location of the individual be public or private. Therefore, the location itself does not determine the applicability of the Fourth Amendment. Instead, the test lies on whether the individual has a reasonable expectation of privacy. Justice Harlan, in his concurring opinion, explained the public has a reasonable expectation of privacy from government surveillance. Accordingly, the use of a cellular phone in a public place does not displace an individual’s Fourth Amendment right to privacy because it is the expectation of this right that courts must consider in the analysis.

While the Court did not engage in a First Amendment analysis, it did recognize the potential need to protect an individual’s public speech. Under the particular facts of this case, the defendant’s freedom of speech would not be protected. However, the Court’s recognition of the potential link between privacy and freedom of speech is important when analogizing cellular phone

---

79. *Id.* at 348.
80. *Id.*
81. *Id.* at 348–49.
82. *Id.* at 351.
83. *Id.* at 360–62.
85. *Id.*
86. *Id.* at 360.
87. *Id.* at 351.
surveillance. Cellular phone surveillance methods encompass a wider range of an individual’s speech than traditional wiretaps. This results in an even greater link between cellular phone surveillance and freedom of speech concerns than wiretapping.

In Katz, the Court also recognized that in times of national security the benefit that a wiretap confers may supersede the Fourth Amendment warrant requirement. An individual’s right to a private conversation under the Fourth Amendment is of paramount importance, and the only time it should be violated is when national security is at stake. Although domestic wiretaps were almost universally accepted for national security purposes, Congress still felt that it was necessary to set legal boundaries that would limit their use. The legislature was concerned about the executive branch’s long-standing use of illegal domestic wiretaps. The safe-guarding procedures Congress imposed were a strong indication that self-governance had failed and that regulation was necessary.

Congress acknowledged the executive branch’s use of unconstitutional wiretapping by enacting Title III of the Omnibus Crime Control and Safe Streets Act (Omnibus Act), which sets strict parameters for domestic wiretapping. These parameters require judicial authorization and define the circumstances in which the court may approve a warrant. The Omnibus Act places restrictions on wiretaps, which include a probable cause requirement and a relevant-to-the-crime requirement. Furthermore, the requesting officer must specify the person under surveillance in the warrant, the location, a description of communications, the name of person requesting, and the length of time. The act limits wiretaps to twenty-six specified crimes, including “murder, kidnapping, extortion, gambling, counterfeiting, and drug-related crimes—all, coincidentally activities associated with terrorist organizations.”

In addition, the Omnibus Act increases the difficulty of obtaining a wiretap to a level more demanding than regular search warrants. In 1972, the Court in United States v. United States District Court, held that warrant-

88. Id. at 359.
89. Donohue, supra note 7, at 1077.
91. See generally id.
92. See generally id.
93. Donohue, supra note 7, at 1078–79.
94. Id.
95. Id.
96. Id.
Inadequate Protections

less domestic wiretapping were not prohibited by the Omnibus Act.\textsuperscript{97} The Court in \textit{U.S. District Court} underlined the importance of freedom of expression, stating that "the potential danger posed by unreasonable surveillance to individual privacy and free expression" could not be preserved if the executive branch had the ability to control domestic wiretap surveillance.\textsuperscript{98} However, the Court's attempt to limit the executive's ability to control surveillance failed, resulting in continued illegal domestic wiretaps without regard to the \textit{U.S. District Court} ruling.\textsuperscript{99}

Wiretapping was the first technology to invade the American citizen's daily life on a massive scale. In 1975, the Church Committee revealed the Government's illegitimate use of wiretaps,\textsuperscript{100} causing American citizens to second-guess the federal government.\textsuperscript{101} Once the Government's unconstitutional use of wiretapping was revealed, the Government was forced to respond and find a workable solution. To solve this issue, the judiciary set precedent to limit the president's domestic surveillance power, while Congress acted to remedy the issue through legislation.\textsuperscript{102}

The Supreme Court has addressed the issue of wiretapping several times. These rulings created a fully-analyzed history of legal and illegal wiretapping, which helped guide the Government's surveillance actions. The Supreme Court clarified that it would not allow unrestricted access via wiretapping into the American public's life.\textsuperscript{103} As with cellular phone surveillance today, wiretapping was the most invasive method of surveillance in its day.\textsuperscript{104}

The wiretapping rulings illustrate the Court's continued belief that the Government's surveillance powers must be regulated. Without statutory limitations to supplement the Constitution, the Government will continue to infringe upon an individual's constitutional rights of speech and privacy. Both the judicial and the legislative branches have taken necessary action to prevent such an infringement,\textsuperscript{105} recognizing a tri-fold system of protection: the Constitution, statutory restrictions, and judicial precedent. Due to the analogous nature of wiretapping and cellular phone surveillance, it would be wise to keep the tri-fold system in place to adequately evaluate cellular phone surveillance and proposed solutions.

\textsuperscript{98} \textit{Id.} at 298.
\textsuperscript{99} Donohue, \textit{supra} note 7, at 1080.
\textsuperscript{100} Dranias, \textit{supra} note 37, at 30.
\textsuperscript{101} See Donohue, \textit{supra} note 7, at 1092.
\textsuperscript{103} \textit{U.S. Dist. Court}, 407 U.S. at 321.
\textsuperscript{104} See Donohue, \textit{supra} note 7, at 1078–80.
IV. THE TECHNOLOGY USED IN CELLULAR PHONE SURVEILLANCE

Cellular phones are inextricably intertwined in Americans' lives. In fact, this intertwining is so profound that cellular phones have practically become a fifth appendage to many people. Indeed, a recent Pew Research survey found the ninety-one percent of Americans own cellular phones. There are two main methods that the Government utilizes to track an individual's cellular phone location: historical data collection and prospective data collection. Now that most of the public carries a cellular device that can track location, new issues related to tracking individuals have arisen.

Acknowledging the suppression of the First and Fourth Amendments by government tracking, Justice Sotomayor remarked, in her concurring opinion of United States v. Jones, that "awareness that the Government may be watching chills associational and expressive freedoms. She further stated that the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." Further, "GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and Government in a way that is inimical to democratic society.'"

A. The Collection of an Individual's Location Through Historical Location Data

The Court's fear that surveillance chills free speech is unprecedented. Recent investigations have revealed that the Government is taking advantage of the historically-low evidentiary bar to perform surveillance by tracking a cellular phones location. In 2011, approximately 1,300,000 requests from law enforcement for cellular phone tracking were processed. These re-


107. Andrew Crocker, Trackers That Make Phone Calls: Considering First Amendment Protection for Location Data, 26 HARV. J. L. & TECH. 619, 625 (2013). Notably, these methods do not take into consideration the Government's additional ability to track an individual through a website's IP address when using a cellular phone's Internet. This technique is not considered because it is not exclusive to cellular phones; any device with access to the Internet can be used to trace the location of an individual through an IP address, whereas the collection of historical information and prospective data is specific to cellular phones.


109. Id. at 956 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

110. Crocker, supra note 107, at 624.

111. Id.
quests utilize a method that produces a “data dump” of location information that encompasses a great amount of citizen’s information by treating both innocent individuals and suspects alike.112 A data dump occurs when the Government obtains a valid warrant for a particular suspect that was in a populated area at the time of the crime.113

This warrant is used by cops in order to obtain the location of a suspect and of an innocent individual who happens to be in the vicinity of the suspect at the time of the crime.114 “Cell sites automatically collect data during normal usage, cellular providers accumulate logs (‘call detail records’) linking specific subscriber accounts, call and Internet connection data, and the nearest cell sector or base station.”115 These “records can, at the least, be used to determine that a user is located within a certain radius of the cell site at a specific date and time.”116 For example, if a suspect were believed to be at a Ku Klux Klan meeting, a cellular data dump would reveal the suspect’s location and the location of all the attendees that had cellular phones.

Recently in Riley v. California, the Supreme Court stated that “location information is a standard feature on many smart phones and can reconstruct someone’s specific movements down to the minute, not only around town but also within a particular building.”117 The Court recognized that cellular phones enable the Government to track intimate details of an individual’s life, stating that “[b]efore cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.”118 Now, however, “a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record.”119 In addition, “a cell phone’s capacity allows even just one type of information to convey far more than previously possible. The sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions.”120 However, “the same cannot be said of a photograph or two of loved ones tucked into a


113. Id. at 515 (noting that the Jones case was only before the court because there was not a valid warrant).

114. Crocker, supra note 107, at 627.

115. Id. at 625–26.

116. Id. at 626.


118. Id. at 2489.

119. Id. (emphasis added).

120. Id. (emphasis added).
wallet.” Notably, “the data on a phone can date back to the purchase of the phone, or even earlier.” While “[a] person might carry in his pocket a slip of paper reminding him to call Mr. Jones[,] he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.”

Finally, there is “an element of pervasiveness that characterizes cell phones but not physical records.” Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception.” This potential invasion of privacy is an obvious infringement upon the Fourth Amendment right to privacy and its underlying First Amendment concerns. The ability of the Government to track an individual’s text messages and emails directly relates to the freedom of expression and speech.

A data dump provides detailed location information about all the individuals within close proximity to the suspect, most of who will never know of the invasion or have a chance to protest against it in court. A data dump impinges upon an innocent individual’s constitutional rights by treating them as if they were criminals. Historical location tracking received its name because this tracking is only retroactive and does not contemporaneously monitor an individual’s movements. However, every time an individual’s cellular phone passes a cellular phone tower, the phone sends a notification to the cellular phone tower and then to the provider alerting that the phone is within the vicinity.

Cellular tower dumps have the ability to reveal an enormous amount of private details regarding an individual’s communications and associations. Visualize the cellular tower as a bucket that is dipped into a pond of water full of guppy fish that represent cellular phone users. The Government

121. *Id.* (emphasis added).
122. *Id.*
124. *Id.* at 2490 (emphasis added).
125. *Id.* (emphasis added).
126. *Id.* at 2488–89.
129. *Id.*
131. *Id.*
132. *Id.* at 627.
chooses to use a huge bucket that catches hundreds of guppies, while only needing to catch one. The Government could choose a smaller bucket to capture the guppy, but a larger bucket is selected because there is no law limiting the use of a large and over-encompassing bucket.133

It is human nature to want more for less. The Government logically fills the larger bucket since current law does not limit the Government’s ability to collect information regarding a criminal investigation.134 This extreme opportunity for invasion into an innocent individual’s private life and association raises concern. It is not a matter of if, but when, the Government will use the association information to its unfair advantage. For these reasons, Congress and the Supreme Court must address this issue through the enactment of statutes along with supporting judicial precedent.

B. The Detection of an Individual’s Location Through Prospective Data Collection

The second method that the Government currently uses to collect surveillance through cellular phones is prospective location data.135 Prospective location data is taken directly from the cellular phone provider.136 In contrast to historic data collection, prospective data collection is conducted concurrently with collection of the user’s location.137

Prospective data collection enables the Government to actively generate and track an individual’s movements. For instance, the Government will ask the cellular phone provider to ping an individual’s cellular phone to transmit the device’s location to the provider who will then transmit it to the Government.138 The use of prospective data collection does not pose the issue of a mass collection of individual locations like it is with cellular tower dumps. However, the greatest disadvantage to prospective data collection is that it requires that an entity know the cellular phone number and provider of the individual.139

C. The Creation of a Highly-Detailed Mosaic Image of an Individual’s Location Through the Use of Both Historic and Prospective Data Collections

When the Government combines multiple data collections and retraces an individual’s steps, creating a detailed map of his whereabouts, a “mosaic

133. See infra Section V.
134. See infra Section V.
135. Crocker, supra note 107, at 627.
136. Id.
137. Id.
138. Id.
139. Id.
map” results.140 This technique was discussed in United States v. Rigmaiden, where the Government created a virtual map of the accused activities and used this image to obtain a conviction at trial.141 The advanced mosaic map, created by the combination of historical and prospective data, is shockingly detailed and permits the Government knowledge of intimate, private communications and associations of the individual’s life.142

Importantly, this specific procedure is reserved for criminal suspects. However, it is possible to include innocent individuals’ data into these data maps by collecting data inaccurately or by the Government’s use of the technology for an ulterior purpose.143 If this occurs then a mosaic map would be a highly detailed cellular tower dump, and innocent individuals would be deprived of their First and Fourth Amendment rights. The mere existence of the technology does not mean that it will be used in a negative manner. However, to best protect the citizens of the United States, the Government has the responsibility to take affirmative steps to limit the availability of a negative use—whether or not it has been utilized.144

V. THE CURRENT LAW LIMITING THE FEDERAL GOVERNMENT’S ABILITY TO PERFORM CELLULAR PHONE TRACKING AND DATA INVASION

The current laws are insufficient to protect the tracking and data invasion of an individual’s cellular phone. Protection from tracking and data surveillance stems from three sources: (1) the First Amendment; (2) Fourth Amendment; and (3) the Electronic Communications Privacy Act (ECPA). These sources are inadequately defined and do not protect Americans from the invasive surveillance that occurs from government meddling.

A. The First Amendment

Usually, the First Amendment is associated with the freedoms of speech, press, religion, and assembly.145 While these rights are no less deserving in modern times, they are not of urgent concern. The last 200 years of First Amendment interpretations have shown the importance of the right to express oneself through oral and written word. The Supreme Court has spent a significant portion of its docket working through classic First Amendment concerns, such as those presented in New York Times Co. v. Sullivan and

140. Id. at 628.
142. Crocker, supra note 107, at 628, n.66.
143. Id. at 634; see also Sinha, supra note 52, at 896.
144. In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1016 (Foreign Intelligence Survey Ct. of Review 2008).
145. See U.S. CONST. amend. I.
Inadequate Protections

Inadequate Protections

Citizens United v. Federal Election Commission.146 However, because cellular phone surveillance has enhanced the Government’s ability to track an individual’s movements, this technology challenges the First Amendment’s ability to protect an individual’s rights to assemble in a whole new way.

The First Amendment states that “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.”147 The Constitution reserves to the people the right to assemble in a peaceful fashion. However, this right is impeded when the Government constantly surveils.148 The Government’s ability to monitor and record an individual’s location creates the opportunity for the individual’s association and assembly activities to be infringed.

Currently, neither Congress nor the Supreme Court has had an opportunity to address the effect that the determination of an individual’s association through location information has on the First Amendment. However, in Citizens United v. Federal Election Commission, the Supreme Court discussed the importance of interpreting the First Amendment in a way that allows it to apply in a variety of situations.149 The Court remarked that the First Amendment is best interpreted when it is given “breathing space” to properly adapt to an ever-changing field of law.150

Under a loose constructionist view of the Constitution, the Constitution itself would be able to conform to new issues that may violate the First Amendment. Therefore, it is foreseeable that the First Amendment itself would restrict the Government’s ability to monitor the public through cellular phones. On the other hand, a strict constructionist interpretation of the Constitution provides little to no protection from the Government’s invasion through cellular phones. While these interpretations lead to drastically different outcomes, neither sufficiently protect a citizen’s privacy. Even the loosest interpretation of the First Amendment would still be limited to varying interpretations of the words of the Amendment. Thus, it is the words of the First Amendment itself that limit its applicability to technological issues and create an impermissible barrier that can only be resolved by a congressional statute addressing these issues.


147. U.S. Const. amend. I.

148. See id.

149. Citizens United, 558 U.S. at 329.

150. Id.
B. The Fourth Amendment

The Fourth Amendment was created to protect an individual’s right to privacy, and once was seen as the beaconing light for that protection.\textsuperscript{151} However, it has now faded into an inadequate safeguard. In fact, some courts have found that, since an individual should not “reasonably expect” privacy while using their personal phone, the Fourth Amendment does not protect the acquisition of location data at all.\textsuperscript{152} While the logic behind the theory that the Fourth Amendment is not infringed when the Government acquires location data seems sound, it crumbles on itself with the realities of tracking technology and the Government’s long-reaching arm. The decrease in constitutional protection, combined with the conflicting judicial interpretations of whether the Fourth Amendment is violated by the interception of location information, highlights the need for a reexamination of the current laws.\textsuperscript{153}

One plausible explanation for this decrease in protection is the ever-changing idea of property. Originally, the “property” that the Fourth Amendment sought to protect was physical property, such as a house.\textsuperscript{154} But today, advancements in law and technology have evolved the concept of property into an entity that was unimaginable at its creation. Particularly, the clause that provides protection for Americans to be “secure in their persons, houses, papers, and effects” at most envisioned the protection of the highest form of invasion at that time: looting and rummaging through an individual’s home.\textsuperscript{155} A pragmatic approach to the Constitution suggests this Constitutional protection was intended to expand with the progression and evolution of America. Such a theory is bolstered by considering that the revolution leading to our advanced technology was unthinkable by the Founding Fathers and consequently left unaddressed.

The Fourth Amendment’s inability to conform to the modern American society is nonsensical; it requires no more to search an individual’s trunk than it does to track an individual’s exact location. This flawed result occurs from the Fourth Amendment’s language that requires a warrant only to search an individual’s exact location. This blanket warrant requirement fails to consider the necessity of tailoring protection to different forms of property, which produce

\begin{itemize}
\item \textsuperscript{151} U.S. Const. amend. IV.
\item \textsuperscript{153} See id.
\item \textsuperscript{154} See U.S. Const. amend. IV.
\item \textsuperscript{155} Id.
\item \textsuperscript{156} Id.; see United States v. Graham, 796 F.3d 332, 345 (4th Cir. 2015); see also United States v. Davis, 785 F.3d 498, 513 (11th Cir. 2015); Woodley, No. 13-113, 2015 WL 5136173, at *9.
\item \textsuperscript{157} See generally id.
\end{itemize}
varying degrees of constitutional infringement. To have the same low standard to acquire a warrant for an individual’s file cabinet as for their physical body seems illogical and unethical considering the massive amount of innocent individuals that are incidentally swept up in the process. Yet, nothing prohibits these types of government action since the Fourth Amendment uniformly applies to all actions.

The evolution of cellular phone tracking is a pivotal issue with federal courts continually analyzing the complexity of a Fourth Amendment violation due to cellular location tracking with and without a warrant. At its creation, the Fourth Amendment was only, and could only be, drafted to protect the property concerns of the day, such as a chair, cabinet, or house. This elementary protection is key to understanding the creation of the Fourth Amendment and the reason why it is no longer providing Americas with the needed protection in the world of technology.

C. Electronic Communication Privacy Act

After severe privacy breaches from wiretaps, Congress acknowledged the lack of public protection from the advanced surveillance permitted under the Electronic Communication Privacy Act (ECPA). The ECPA was enacted in 1986 under 18 U.S.C. § 2510-22. This Act is composed of both the Electronic Communication Privacy Act and the Stored Wire Electronic Communications Act, which together are singularly referred to as Electronic Communications Privacy Act of 1986. Generally, the ECPA protects wire, oral, and electronic communication when it is created, transmitted, and stored. Notably, this Act is not designed to protect cellular phone surveillance. While this is an interrelated field, the ECPA was enacted at a time when cellular phones were still in a stage of infancy.

The ECPA controls the Government’s ability to compel cellular phone providers to release electronic communication, such as calling records. Although the ECPA is a step in the right direction to provide adequate protec-

158. See Graham, 796 F.3d at 345–51; see also Woodley, No. 13-113, 2015 WL 5136173, at *9.
161. Electronic Communications Privacy Act of 1986, JUSTICE INFORMATION SHAR-
tions with respect to cellular phone surveillance, over time two critical structural issues have appeared. First, "the frequency with which the Government obtains orders under inconsistent (and relatively undemanding) standards. Second, the secrecy and lack of review surrounding these orders." 165

The ECPA is plagued with unworkable issues. For instance, the ECPA requires reasonable suspicion or probable cause to obtain location information, but the definition of either standard is not understood. 166 In addition, there is confusion as to what standard the Government must meet when seeking to obtain location information as the ECPA does not apply directly to cellular phone technology. 167

It is likely that the Government files the majority of requests under the less stringent standard of reasonable suspicion. 168 This is not surprising because logically, when providing two standards and when one is more easily satisfied than the other, there will be a higher usage of the easier-to-meet standard. This leads to inconsistency and unfairness in the ECPA’s application. "The inconsistent and increasingly fractured standards for obtaining location data under ECPA have led commentators and civil liberties groups to bemoan the state of the law and call for judicial and legislative reform." 169 As a solution to this inconsistency, the Supreme Court should "require probable cause, or Congress could add language codifying the forms of location data and clarifying more specific application of ECPA authorities." 170 This would eliminate the Government’s ability to select a less rigorous standard, thus creating a uniform and a fair application of the ECPA. 171

In addition, the ECPA does not require that the Government notify the individual whose activity is being monitored. 172 There are two issues that arise from this “secret” surveillance. First, there lack of legal notice to the victim. Throughout cellular phone surveillance is the lack of judicial protection provided to an individual due to the lack of notice required to file a suit. 173 Thus, a circular reaction occurs from the lack of notice given to individuals by producing a lack of judicial progress governing cellular phone technology. This is because litigants are not able to bring a suit, which shows the Government’s deliberate ignorance of constitutional infringement. Sec-

165. Crocker, supra note 107, at 630.
167. Crocker, supra note 107, at 630.
168. Id. at 631.
169. Id. at 633.
170. Id.
171. Id.
172. Id. at 634.
173. Crocker, supra note 107, at 634.
ond, surveillance conducted in secret decreases in public discourse about these methods.174

The 111th Congress addressed the need for electronic privacy reform by amending the ECPA because, in its current state, it lacks the level of protection required to safeguard citizen’s rights in the digital age.175 Congress designed the ECPA to protect a citizens’ use of electronic devices, but as digital devices evolved, Congress has failed to reform the ECPA accordingly.176 The chairman of the committee assigned to address the reformation of the ECPA remarked "bringing this privacy law into the digital age will be one of Congress’s greatest challenges."177 He further explained that the law is plagued with many conflicting standards that create uncertainty in its application.178 While nearly five years have passed since the acknowledgment of the ECPA’s inadequacy, Congress has not yet attempted to fix these issues through reform.179

The First and Fourth Amendments, as well as the ECPA, were enacted prior to the development of cellular phones and, therefore, none of these expressly apply to cellular phone technology.180 It is necessary that Congress affirmatively enact new laws to further Constitutional protections in this area. A law that clearly extends the rights of the First and Fourth Amendments through judicial action, and congressional enactment of law with the Amendments’ underlying policy concerns of public discourse, public congregation, and privacy of communication will efficiently and effectively correct the Constitution’s impeding corrosion. An essential aspect of the U.S. government is the ability for the Constitution to adapt to an evolving society and for Congress to enact statutes where the Constitution does not speak.181

D. Benefits of the Government Tracking Cellular Phones

There are legitimate purposes for tracking cellular phones, but tracking technology must be limited to emergency and statutorily approved purposes. Tracking technology can serve the legitimate purpose of keeping individuals

174. Id. at 639.


176. Id.

177. Id.

178. Id.


180. Crocker, supra note 107, at 631.

safe in the event of an emergency. For example, emergency responders are able to locate an individual because of the Federal Communication Commission rule that requires a precise location in emergency situations. The idea behind this requirement is that in an emergency situation, a cellular phone is likely to be with the individual and the ability to expeditiously locate their cellular phone could save lives. According to current laws, the Constitution is not unreasonably threatened by the use of this technology for an emergency situation. However, the use of this same technology for a different purpose, such as locating a suspect, risks violating an individual’s constitutional rights.

VI. ENACTMENT OF A STATUTE IS THE BEST SOLUTION TO DETER INFRINGEMENT OF FIRST AND FOURTH AMENDMENT RIGHTS

Because currently the laws enacted inadequately protect individual’s First and Fourth Amendment rights, Congress has an obligation to remedy these issues. In fact, federal circuit courts have recognized the need for legislative reform while making the grim constitutional rulings. For instance, in Davis, the Supreme Court stated,

[P]roposals should be directed to Congress and the state legislatures rather than to the federal courts. As aptly stated by the Fifth Circuit, “the recourse for these desires is in the market or the political process; in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections.

Neither the Constitution nor the ECPA adequately addresses the issue of cellular phone’s invasion into American lives. The problem created with cellular phones is too unique and complex of an issue to be addressed by statutes indirectly. In the past, statutes that have looked to fix this issue have done so by compiling it with other electronic issues. However, a statute

182. Crocker, supra note 107, at 626.
183. Id.
184. Id.
185. Id. at 622.
186. Id. at 637.
187. See id. at 630.
188. United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015).
189. Id.
190. Crocker, supra note 107, at 630.
191. See Electronic Communications Privacy Act of 1986, supra note 161 (establishes that the ECPA applies to email, telephone, and data stored).
must address this issue specifically in order to respond to the complexity of cell phone surveillance.

A statute that focuses solely on cellular phones needs to be enacted. It should focus on the ability of cellular phones to track the location of an individual and limit the Government's ability to obtain this information. This would not be the first time that Congress used a statute to focus solely on one form of technology. The Omnibus Bill for example, focused solely on wiretaps.\(^{192}\) Thus, Congress is urged to act in accordance with its procedure in addressing wiretaps. In that instance, Congress recognized the gap in applicable law and its need to remedy the issue. Enacting a statute for cellular phone surveillance does not require too much of Congress in their representation of the American public.

There are egregious wrongs that occur as a result of tracking an individual's location and Congress has the responsibility to fix this issue in order to fulfill their obligation to the American public. The Fourth Amendment is clearly infringed by the direct invasion of an individual's privacy when their cellular phones are tracked.\(^ {193}\) Further, the First Amendment is indirectly infringed upon when the Government compiles the location of an individual because the location of an individual reveals their association.\(^ {194}\) The proposed name for this bill is The National Cellular Tower Surveillance Act (NCTSA). Limiting technology is illogical and not in the best interest of our society. Therefore, the Government must be prohibited from using the technology in an unconstitutional manner.

Under the NCTSA, the Government would be limited in several regards to cellular phone surveillance. In most instances, the Government would be limited to requesting information from cellular phone providers only on suspects to prevent a cellular tower dump. However, if it were necessary for the Government to acquire a mass collection of cellular phone information, then the Government would have to satisfy a higher standard of proof. This directly considers the Government's potential constitutional interference to determine the correct process that it must take to retrieve location information.

---


193. See U.S. Const. amend. IV; see also Crocker, supra note 107, at 634–36 (arguing that the current state of the Fourth Amendment is not adequately protecting against the direct invasion of individual privacy through cellular phone tracking).

194. See U.S. Const. amend. I; see also Crocker, supra note 107, at 636 (arguing that First Amendment rights may be implicated when tracking cellular phone activity).
A. Substantive Solution

Under the current law, the standard of proof to obtain a warrant is probable cause.\textsuperscript{195} However, due to the high possibility that constitutional infringement can occur from tracking cellular phones, a higher standard should be adopted. Raising the standard of proof for cellular tracking is necessary in order to protect the public from unnecessary searches and seizures. This solution proposes that a court weigh the Government’s interest in tracking with the individual’s constitutional right to both privacy and anonymous association. This requires a dramatic change from the current standard, which only requires the Government to show that there is some evidence to support the acquisition of the information.\textsuperscript{196} The change in the standard of proof will faithfully guard an individual’s privacy and right to free speech.

In fact, the increased standard of proof aligns with the Government’s standard of proof for First Amendment violations.\textsuperscript{197} The Supreme Court holds that for the Government to infringe upon the First Amendment by revealing the membership list of an organization it must prove to have a compelling interest in the revelation.\textsuperscript{198} Clearly, raising the standard of proof needed to acquire location information, which could potentially infringe upon an individual’s constitutional rights, is nothing new.

Notably, precedent has shown that a higher standard is normal and advisable. For instance, the standard for the NCTSA lies between the probable cause standard and the without a reasonable doubt standard. A fusion of these standards would require a more thorough analysis before granting permission to collect innocent individuals’ location data, while also providing a manageable standard when a cellular tower dump is legitimately needed to capture a suspect. Similar to the Omnibus Act’s provision, this standard is kept practical by only increasing the burden of proof when innocent individuals are involved.\textsuperscript{199} The Government’s procedure will only require a higher standard in those cases where more than a suspected individual could fall victim to unconstitutionality. In all other cases, the Government will follow the procedure already in place.

In the alternative, if Congress believes it too burdensome to require a higher burden of proof, then a detailed description of additional procedural requirements, as in the Omnibus Acts, should be a part of the NCTSA.\textsuperscript{200} This list would outline the step-by-step procedure that the Government must follow to acquire location information. This guide would help solve some of

\textsuperscript{196} Id.
\textsuperscript{198} Id.
\textsuperscript{199} See Title III of the Omnibus Crime Control and Safe Streets Act of 1968, supra note 192.
\textsuperscript{200} Id.
the uncertainty in the ECPA. The NCTSA would effectively and properly balance the innocent persons First and Fourth Amendment rights and the Government’s interest in apprehending suspects. It will also create the opportunity for Congress to address analogous issues with cellular phones, such as data invasion, in the future. Because of the current laws inconsistencies and inefficiencies, Congress is urged to enact a comprehensive statute that directly addresses the issue of broad cellular tower dumps infringing upon the First and Fourth Amendments.

B. Procedural Solution

Another hindrance to bringing a claim against the Government’s invasion of an individual’s First and Fourth Amendment’s rights through cellular phone tracking is the inability to establish notice, standing, and a proper remedy, which are all required to bring suit. If the Government restricts an individual’s access to any of these three requirements, a suit for breaching an individual’s constitutional right can never be brought.

i. Notice

Since the Government does not notify each individual whose data is swept up in a cellular tower dump that their location data has been revealed, the individual does not have notice.201 Without bringing this information to the individual’s attention, the Government violates that person’s rights because they are unaware of the potential for a suit on constitutional grounds.202 Because of the large quantity of information received through cellular tower dumps, it seems neither efficient nor effective to require the Government to notify each individual of the dump. But if the Government did notify each individual, the amount of suits actually brought will likely be lower. However, regardless of the inefficiency, individuals lack the notice necessary to challenge the acquisition of their location data in court.203

ii. Remedy

Even in the rare event an individual is given notice of location tracking, he or she “can only challenge the use of this data to the extent that existing law provides a remedy.”204 It seems that, under current law, there is not a proper remedy for the courts to award. The ECPA does not provide a remedy to suppress the use of location data, thereby directly contradicting the American judicial system by leaving citizens without a method of relief.205 The likely remedy under the current law would be for the individual to seek an

201. Crocker, supra note 107, at 639.
202. Id.
203. Id.
204. Id. at 639.
injunction against the Government to prevent further invasion. However, the NCTSA should provide whatever relief Congress deems necessary.

iii. Standing

In addition to notice and remedy, the standing doctrine is also a barrier to a First and Fourth Amendment claim. Historically, standing is an issue for an individual that wants to bring a constitutional claim. Generally, this is because a constitutional issue often applies to a wide variety of individuals without an obvious injury. Regardless of the difficulty in establishing standing, the Supreme Court and Congress have not addressed this hurdle.

To satisfy the standing requirement, a plaintiff must bring a claim that shows harm. The dichotomy in interpreting standing is provided in Laird v. Tatum, which further explains the issue with the standing doctrine. The narrow interpretation of standing in Laird is to view the reduction of free speech as a harm to establish standing. However, the actual application of the holding by lower courts shows a different interpretation and allows for the reduction of free speech to satisfy the standing requirement.

The Supreme Court has acknowledged that a concrete injury sufficient to satisfy the standing requirement results from a drop in active participation and membership. In Socialist Workers Party v. Attorney General, Justice Marshall accuses the Government of applying the Laird holding too broadly and asserts that an injury, such as membership loss, is sufficient to overcome the procedural threshold issue. Thus, the litigants need only show, through objective data, that an action taken by the Government has affected its organization's membership or attendance numbers. If this form of harm is recognized, the claim is more viable because the chilling of speech and the decrease of membership in an association are likely results of the Government's invasion on speech and privacy.

After satisfying these three procedural issues, there is the question of whether the Supreme Court would even consider addressing the issue. The

---

206. Id.
207. Crocker, supra note 107, at 640.
208. Id.
209. Id.
211. Crocker, supra note 107, at 639–40 (citing Laird v. Tatum, 408 U.S. 1, 15 (1972)).
212. Id.
213. See ACLU v. NSA, 493 F.3d 644, 660 (6th Cir. 2007); see also United Presbyterian Church v. Reagan, 738 F.2d 1375, 1378 (D.C. Cir. 1984).
215. Id.
Court limits its review of constitutional issues by narrowly construing the question of certification. Historically, the Court has avoided addressing a constitutional issue by resolving the problem on other grounds. It is these bleak conditions that an individual must face to even have the opportunity to have the Court address the protection of their constitutional rights in the modern world of cellular phone surveillance.

After recognizing the many barriers one must overcome and the confusion within each procedural hurdle, it becomes even more apparent that it is necessary for Congress to enact a precise statutory solution. The enactment of the NCTSA that directly addresses the First and Fourth Amendments should require that the Government to give notice to all individuals, create a statutory remedy, and establish standing when a chilling effect is proven. The NCTSA should give every citizen his or her constitutional right to a day in court.

This Comment urges Congress to follow its precedent of the Wiretapping Act and enact a statute to protect Americans against cellular phone surveillance. While the Court could still deny certification of the issue because a statute that an individual can file suit under exists, it is less likely that the Court will even face the issue. The statute will nip the problem in the bud before it comes to fruition.

A statute addressing this new invasive form of surveillance fits with the natural progression of our society. Just as Congress acted with the Wiretapping Act and it is urged to follow suit with cellular phone surveillance. This progression is logical because the same policy issues faced by the American public with cellular surveillance were faced with wiretapping—invasion of privacy, the ability to reveal anonymity and associational ties, and the potential to chill speech. While these injuries are speculative in nature, these are the exact rights that the Constitution seeks to protect. The Supreme Court has recognized these dangers in Jones and therefore these surveillance methods must be limited. The best form of limitation would be for Congress to enact a statute that directly addresses cellular phone surveillance and the Government’s limitations, much like that of NCTSA.

VII. CONCLUSION

The First and Fourth Amendments of the Constitution were not created to face the issue of cellular phones surveillance. Similarly, the ECPA was only created to protect cellular phone users and does not provide additional protections. Congress has repeatedly recognized the Constitution’s limitation in protecting U.S. citizens’ rights. Congress attempted to regulate other types of technology, but has failed to do so for cellular phones. For instance, the Wiretap Act was enacted to combat the executive branch’s ability to perform


wiretaps. Thus, creating a statute to supplement the Constitution to address the cellular phone surveillance is a natural extension.

While nothing directly precludes the Government's ability to track an individual's location through his cellular phone, the intent of the First and Fourth Amendments directly and indirectly prohibit an unjustified invasion of privacy. The First Amendment embraces an individual's right to speak freely without worrying about negative repercussions and encourages an individual to associate with who he may choose. Further, the Fourth Amendment is meant to protect a citizen's right to privacy. The Fourth Amendment also includes the right to have privacy in one's lives. Congress should fulfill the Founding Fathers' hopes of protecting a citizen's right to privacy and speech by enacting a statute that limits the Government's ability to surveil cellular phones.

Together the First and Fourth Amendment craft a life for every American that can be uniquely his own. The Constitution allows an individual to live exactly how he desires without the fear of reprisal. The ability of the U.S. government to track an individual's movements through a cellular phone directly contravenes this policy. It is the responsibility of Congress to address this issue. The NCTSA should provide the protection that Americans deserve. Hopefully in time, U.S. government will adjust the scales of Lady Liberty to be in favor of the American public.
**APPENDIX A:**

Question: “If the government has the ability to track your personal cellular phone’s location would this lead you to take a second thought about the activities or groups that you chose to associate with?”

<table>
<thead>
<tr>
<th>Age</th>
<th># of Yes</th>
<th># of No</th>
</tr>
</thead>
<tbody>
<tr>
<td>21-40</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>40-60</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>60-80</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>