**WAKING UP FROM WONDERLAND:**
**WARRANTLESS SEARCHES THROUGH MODERN TECHNOLOGY**

GUNTER A. FERNANDEZ

# Table of Contents

INTRODUCTION ..... 13
I. THE BEGINNING ..... 14
II. KATZ AND PRIVACY ..... 15
III. PRIVACY AND EXPECTED PRIVACY ..... 16
IV. TECHNOLOGY AND EXPECTED PRIVACY ..... 18
V. INCLUSION OF TRESPASS ON PHYSICAL PROPERTY ..... 19
VI. TECHNOLOGY AND LOCATION SEARCHES POST-*JONES* ..... 20
VII. REASONABLENESS ELEMENT ..... 25
VIII. GOOD FAITH EXCEPTION ..... 26
IX. LEGISLATIVE ALLEVIATIONS ..... 27
X. SOLUTION PROPOSED ..... 28
CONCLUSION ..... 29

## INTRODUCTION

Texting, e-mailing, updating Facebook statuses, and following twitter feeds describe actions that a great part of the current youth participates in daily. Moreover, for some of us, it is hard to remember a world without basic cell phones, which let us communicate and transfer information in a matter of seconds through wireless signals. Likewise, future generations will not be able to comprehend how people used to live without the modern commodities of smart phones, which let people take pictures, and allow pictures to be shared with hundreds of people, or being able to visually communicate with people around the globe instantly on their mobile devices. Additionally, even now some people depend on their phones or other GPS[1] devices to help them localize where they are when they are lost. Or to find the best route from their location to a place of business that their friends have recommended through their online statuses, and their respective GPS locations.

And yet, these new capabilities contrast with our right to be secure from unreasonable searches, and our notion of privacy. As we are sharing images with our friends, and in some cases with strangers, with these technologies we instantly open our thoughts to the rest of the world. We are also providing our location on a constant basis to third parties, whom can keep a daily surveillance of us.[2] Similarly, we are opening the privacy of our homes and effects through this media, and inviting and authorizing constant surveillance of our private spaces.

However, most people do not think that they are giving up their privacy when authorizing third parties to access their precise locations through their phones, or that we authorize our homes to be effectually bugged[3] when we leave consoles connected to the internet that perform different functions through voice and video recognition. And that is the source of the problem, the shock between what we think needs to be protected from unwarranted searches and our willing exposure of our privacy to third parties, which leaves the door open for government surveillance without warrants.

Consequently, the Supreme Court and lower courts have tried to resolve the issue of our expected privacy and our right granted by the Fourth Amendment to be safe from unreasonable searches.[4] One of the attempts to reconcile the Constitution and the applied law as it relates to modern technology is *United States v. Jones*.[5] In that case, the Supreme Court reintroduced the concept of common law trespass when analyzing the Fourth Amendment. In *Jones*, the Court applied the "right to be safe in their . . . effects" language of the Fourth Amendment to show that the installation of a tracking device on a suspect's car, in order to track his movements, constituted a search.[6]

This Note will identify the main cases that have led to the current interpretation of the Fourth Amendment as it relates to warrantless searches, our expected privacy, modern advances

---

[1] Global Positioning System.

[2] Cellphone companies, security applications, and home security.

[3] A form of electronic surveillance by which conversations may be electronically intercepted, overheard, or recorded, usu. covertly; eavesdropping by electronic means. BUGGING, Black's Law Dictionary (9th ed. 2009), see Bluebook 15.8(a) bugged.

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

[5] 132 S. Ct. 945, 949 (2012).

[6] *Id.*

in technology, and the legal fiction[7] created therein. Then, the Note will illustrate some of the problems and confusion among the courts regarding the application of the Supreme Court's interpretation of the Fourth Amendment. Then, the Note will show how some courts narrowly interpreted the Supreme Court's interpretation of admitting warrantless searches with regard to modern technologies. The Note will then show some legislative solutions that have been created to resolve this issue. The Note will conclude by providing a solution to ease the problems associated with the Supreme Court interpretation of the Fourth Amendment and how courts are applying it.

## I. THE BEGINNING

The Fourth Amendment of the Constitution guarantees the right of people to be free from unreasonable searches and seizures. The Fourth Amendment states that:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[8]

But what exactly constitutes a "search?" The Fourth Amendment has been interpreted in different ways over the last century.[9] And as technology and policing methods for acquiring evidence have modernized, these interpretations protected the privacy of citizens. From the 1920s until the 1960s, it was interpreted to mean that a search took place when there was an actual physical intrusion of property.[10] In *U.S. v. Silverman*, the Court stated that eavesdropping on a conversation with a "spike mike"[11] was a search and required a warrant.[12] In that case, a microphone was placed outside the defendant's living quarters and was used to listen to the conversation inside the home.[13] The Court held that because it was actually physically connected to the defendant's wall, it was a search.[14] The Court focused on the physical intrusion of the government into a constitutionally protected area.[15] However, this interpretation changed as new methods of eavesdropping were developed.

One of the methods used to bypass the physical trespass limitation was tapping the phone line outside of the defendant's property. This was the issue in *United States v. Olmstead*, where the Supreme Court held that there was no search when police tapped phone lines in a public area

---

[7] An assumption that something is true even though it may be untrue made esp. in judicial reasoning to alter how a legal rule operates. LEGAL FICTION, Black's Law Dictionary (9th ed. 2009), legal fiction.

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

[9] *See, e.g.*, Olmstead v. United States, 277 U.S. 438 (1928); Nardone v. United States, 308 U.S. 338 (1939); Katz v. United States, 389 U.S. 347 (1967).

[10] *See, e.g.*, United States v. Silverman, 365 U.S. 505, 506 (1961); *Olmstead*, 277 U.S. at 438.

[11] A spike is a contact microphone for listening through walls.

[12] *Silverman*, 365 U.S. at 512.

[13] *Id.*

[14] *Id.*

[15] *Id. See also*, Boyd v. United States, 116 U.S. 616 (1886).

rather than on the defendant's property, and did not seize a tangible thing.[16] This interpretation of the Fourth Amendment had several limitations, one of which is that it only protects the physical element and not the message being transferred.

## II. KATZ AND PRIVACY

In 1967, the Court changed used a different interpretation in *Katz v. United States*.[17] In that case, the Court introduced the concept that "the Fourth Amendment protect[ed] people—and not simply 'areas'—against unreasonable searches" and that "the reach of [the Fourth] Amendment [could not] turn upon the presence or absence of a physical intrusion into any given enclosure."[18]

Therefore, the Court held that even though the government did not physically intrude into the phone booth where the defendant was speaking, listening to the conversation was a search.[19] Moreover, the Court concluded that "the underpinnings of Olmstead . . . ha[d] been so eroded by . . . subsequent decisions that the 'trespass' doctrine . . . enunciated [could] no longer be regarded as controlling."[20] The Court also stated that "[t]he Government's activities in electronically listening to and recording . . . violated the privacy upon which [the Defendant] justifiably relied."[21] Therefore, the Court redefined its interpretation of the Fourth Amendment, clearly stating that it protected people, not places.[22] This interpretation was a great step forward in protecting the privacy of people, and helped to create a bridge between what the drafters of the Constitution wanted to protect and the exposure created by the use of modern technology.

The *Katz* decision emphasized that people's privacy is protected when their actions were conducted in areas where a person could reasonably expect privacy, and not in public places, thus government intrusion in public places would not constitute a search.[23] Judge Harlan concurred and restated the Court's twofold test for privacy protected by the Fourth Amendment: "first that a person . . . exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[24]

The holding in *Katz* seemed to limit the ability of government to investigate without a warrant, as it narrowed government's ability to collect evidence when a search intrudes on an expectation of privacy that society considers reasonable. Nevertheless, in *United States v. Miller*,[25] the court decided that there was no legitimate "expectation of privacy" in the contents of documents that were voluntarily conveyed to banks, and were also exposed to their employees in the ordinary course of business.[26] In that case, the defendant was convicted of "possessing an unregistered still, carrying on the business of a distiller without giving bond and with intent to

---

[16] *Olmsted*, 277 U.S. at 466.
[17] 389 U.S. 347 (1967).
[18] *Id.* at 353.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.* at 466.
[24] *Id.* at 361.
[25] 425 U.S. 435 (1976).
[26] *Id.* at 442.

defraud the Government of whiskey tax, possessing 175 gallons of whiskey upon which no taxes had been paid, and conspiring to defraud the United States of tax revenues."[27]

In the defendant's trial, the State introduced evidence of bank account records and checks that were used to pay for the materials and the paraphernalia to distill alcohol.[28] The defendant appealed the conviction on the ground that the bank documents were illegally seized.[29]

The Court of Appeals agreed with the defendant, stating that the information obtained should not have been admissible as the subpoena was faulty and the acquisition of the records violated the defendant's Fourth Amendment rights; nevertheless, the Supreme Court reversed the decision.[30] The Court held that there "was no intrusion into any area in which respondent had a protected Fourth Amendment interest."[31] The Court explained that the "Fourth Amendment [did] not prohibit the obtaining of information revealed to a third party" which was then conveyed by the third party to Government authorities.[32] The Court stated that "even [when] the information [was] revealed on the assumption that it [would] be used only for a limited purpose and . . . confidence [was] placed [o]n the third party . . . ." it could not protect the information if it was willingly given it by the third party.[33]

## III. PRIVACY AND EXPECTED PRIVACY

The *Miller* decision was an important step in re-opening the government's ability to gather evidence when it lacked probable cause to obtain a warrant. The Court redefined this concept in *Smith v. Maryland,*[34] where it explained how revealing information to third parties could apply to the evolving technology of the late 1970s.

In *Smith,* the Court decided that the installation and use of a pen register[35] did not constitute a search within the meaning of the Fourth Amendment.[36] The defendant In that case, the defendant robbed and harassed an individual.[37] After the robbery, the defendant continued to pester the victim through threatening and obscene phone calls.[38] When the police located a vehicle that met the defendant's car description, the police traced the license plate number, and were then able to identify the defendant. At that point, the police asked the phone company to install a pen register to record the numbers dialed from the defendant's phone.[39]

---

[27] *Id.*
[28] *Id.*
[29] *Id.* at 438-389. (The subpoena that was used to obtain the records was invalid, and the information obtained through the invalid subpoena constituted a violation of the defendant's Fourth Amendment rights).
[30] *Id.* at 446.
[31] *Id.* at 440.
[32] *Id.* at 443.
[33] *Id.*
[34] 442 U.S. 735 (1979).
[35] A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed. *United States v. New York Tel. Co.*, 434 U.S. 159, 161 n.1 (1977).
[36] *Id.* at 736.
[37] *Id.* at 737.
[38] *Id.*
[39] *Id.*

The warrantless pen register revealed that the defendant had called the victim, which then led to a warranted search of the defendant's property.[40] In his trial, the defendant moved to suppress all of the evidence obtained through the pen register, but the court denied the motion because the court held that the defendant did not have any legitimate expectation of privacy in the phone numbers that he dialed because the records were held by a third party.[41] The defendant was then convicted and sentenced to six years in prison. In all of the defendant's appeals the lower courts stated that the installation of the pen registers was not a violation of his Fourth Amendment rights.[42]

The Supreme Court stated that the defendant did not have an expectation of privacy in the phone numbers that he had dialed; moreover, the Court stated that even if he did, his expectation was not a "legitimate" expectation of privacy.[43] The Court first reasoned that telephone users generally do not have any expectation of privacy regarding the numbers they dial, since it was known that the dialed numbers were conveyed to the telephone company.[44] Furthermore, the Court stated that users knew that the phone companies had facilities for recording the information.[45] Users also knew that the companies did in fact record the numbers dialed for various legitimate business purposes such as to check bills and price rates, as well as detect fraud and prevent violations of law.[46]

Moreover, the Court stated that even if the defendant had a subjective expectation of privacy, that expectation was not one that society was prepared to recognize as "reasonable."[47] The Court stated that because the police installed the pen register on the phone company's property, the defendant could not claim that this property had been invaded or that police had intruded into a "constitutional protected area."[48]

However, in *Smith* the Court stated that due to the pen register's limited capabilities, in that it could not pick up or record sound, the defendant could not argue that it intruded into a private conversation.[49] *Smith* set a precedent for similar cases that have arisen because defendants gave implied or actual permission to third parties to access private areas and information. Nevertheless, *Smith* is different from most of the modern privacy problems because now individuals voluntarily post information to a wide variety of third parties and give explicit permission to companies to collect the information. For example, the permission we give to our phone provider to use the phone's GPS and track our family members in real time through their website, as well as the permission we give to other companies that allowed us to use the phone's GPS to find the current location of our lost or stolen phones. Likewise, we also provide permission to companies that provide home security to access cameras from the interior of our homes for monitoring purposes, as well as the access we provide to internet servers that allows

---

[40] *Id.* at 739.
[41] *Id.* at 745.
[42] *Id.* at 740.
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.* at 741.
[49] *Id.*

us to observe our pets while we are away. Similarly, we also provide an implied permission when we broadcast videos from our homes.

## IV. TECHNOLOGY AND EXPECTED PRIVACY

The interpretation of "reasonable search" that was set forth in *Katz* was used in the 1980s in both *United States v. Knotts* and *United States v. Karo*.[50] In *Knotts*, the Supreme Court decided whether the placement of a radio transmitter without a warrant constituted an unreasonable search.[51] In that case, a transmitter was placed inside a chloroform container before being sold to the defendant; the transmitter was used to track the container.[52] However, the officers also visually followed the containers.[53] The Court considered the legitimate expectation of privacy interpretation of the Fourth Amendment and held that the search was not unreasonable because the officers visually tracked the containers and their movement through public roads.[54] The Court focused on the issue that arose in both *Smith* and *Miller* that focused in the fact that since the defendants had exposed themselves to the public they could not expect any privacy. In *Knotts*, the Court slightly evaded the question regarding the admission of evidence and the use of technology by indicating that as long as there was a valid alternative,[55] the evidence would be admitted. This solution did not reconcile the law and expectation of privacy through the use of technology.

However, in *Kyllo v. United States* the Court did address the issue of whether advanced technology could be used not to observe what a defendant might expose to the world voluntarily, but what a defendant would consider to be private.[56] In that case, the Court decided that the use of thermal imaging devices was a search and required a warrant.[57] Because the use of thermal imaging technology was not used by the public, using that technology constituted a search and a warrant was therefore required.[58] Likewise, the Court considered the intrusion posed by that particular technology, and the issue as to whether there should be a distinction between through-the-wall technology and off-the-wall technology.[59] However, the Court concluded that even off-the-wall technology invaded an individual's privacy.[60] The Court reached this decision by considering the special aspects of that situation, such as the breach of privacy to the defendant's dwelling, which the Court had previously held as a highly protected area from unwarranted searches and privacy intrusion. The Supreme Court's ruling in *Kyllo* strengthened the position that a person's privacy expectation in his home was an area deserving of a high level of protection, even when the individual unintentionally exposed his actions in the home by

---

[50] United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276, 277 (1983).
[51] *Knotts*, 460 U.S. at 277.
[52] *Id.*
[53] *Id.*
[54] Kyllo v. United States, 533 U.S. 27, 29 (2001).
[55] In this case, the alternative way of acquiring the evidence was through the visual surveillance that the officers maintained throughout the investigation.
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] Thermal imaging only looks at the heat emitted from the wall, and therefore does not invade the internal area of a home.
[60] *Id.*

generating heat. Thus, courts have used this interpretation to resolve similar issues relating to warrantless searches and unintentional home exposures through technology.

In *United States v. Wahchumwah*,[61] the Ninth Circuit held "that an undercover agent's warrantless use of a concealed audio-video device in a home into which he has been invited by a suspect [did] not violate the Fourth Amendment." The court applied the principles set forth in both *Katz* [62] and *Hoffa*[63] to reach its decision.

In *Wahchumwah*, the prosecution offered evidence at trial that was obtained by using concealed audio and video devices attached to an undercover agent. The defendant was then convicted for violating the Bald and Golden Eagle Protection Act, and for selling and offering to sell both tails and plumes of Golden Eagles. On appeal, the defendant argued that the warrantless use of the audio and video devices violated his Fourth Amendment rights by infringing on his privacy interest. Moreover, the defendant argued that the use of a video camera in his home was similar to *Jones*, in that there was a physical violation of his home, and that it was similar to *Nerber*, where the use of a video camera violated his expectation of privacy.

However, the Ninth Circuit disagreed. The court relied on the principles set forth in *Katz*, and then reinforced by *Hoffa*, by stating that the defendant did not have an expectation of privacy since he had knowingly exposed the interior of his home to the undercover agent. The court also emphasized that it did not matter that the defendant did not know it was an agent to whom he had exposed his home, nor that the method of recording the information was through video and audio.

*Wahchumwah* is distinguishable from *Kyllo* because the defendant in *Wahchumwah* voluntarily exposed the contents of his home when he invited the undercover agent in, while the suspect in *Kyllo* did not invite the government to enter his home to look around, and therefore had no reason to suspect that such an inspection was even possible. Likewise, in *Nerber*, the court rejected the defendant's claim that this surveillance was unconstitutional because business visitors to a hotel room had a reasonable expectation that they would not be videotaped when their guest left the room.

## V. INCLUSION OF TRESPASS ON PHYSICAL PROPERTY

The interpretation of the Fourth Amendment was drastically modified once again in *United States v. Jones*. In that case, the Court reconsidered the clause of "[t]he right of people to be secure in their . . . effects, against unreasonable searches" of the Fourth Amendment[64]; a factor which had been omitted in preceding cases to determine whether a search had occurred.[65] In *Jones*, the Supreme Court decided that the placement and use of a GPS device on the defendant's vehicle constituted a search.[66] The police had acquired a warrant for the use of the GPS, but when the police installed the GPS on the defendant's vehicle the warrant had expired.[67]

---

[61] 2012 WL 5951624 (9th Cir. 2012).

[62] Expectation of privacy does not extend to "[w]hat a person knowingly exposes to the public, even in his own home or office." *Katz*, 389 U.S. 347 at 351.

[63] Defendant generally has no privacy interest in that which he voluntarily reveals to a government agent. *Hoffa*, 385 U.S. at 300–02.

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

[65] *Jones*, 132 S. Ct. at 946.

[66] *Id.*

[67] *Id.*

Moreover, the installation of the GPS was done in a different state than the warrant was issued. The prosecutor argued that the use of the GPS was not a search based on the prior interpretation of the Fourth Amendment.[68] However, the Court expanded the prior interpretation, by explaining that the case did not fall under the "Katz formulation."[69] The Court resolved the case by stating that the government's physical intrusion on an "effect"[70] for the purpose of obtaining information constituted a "search."[71] Furthermore, the Court explained that the test did not replace the previous *Katz* analysis but that it was an addition to that test.[72] And even though the Court concluded that the method of obtaining the evidence indeed constituted a warrantless search, the analysis that the court used was similar to the analysis of *Knotts.*[73] This was a clever solution for the court, for if the court had relied on the *Kyllo* analysis in this case, the use of a GPS would not have been considered a violation of the Fourth Amendment. GPS technology is widely available and used by the public; therefore, the advanced technology argument would not have been an effective way to protect the expected privacy of the defendant. However, despite this ingenious solution, the Court still left open a gap between the uses of technology that does not trespass on the defendant's person, property, or effects, but that society holds with an expectation of privacy.

## VI. TECHNOLOGY AND LOCATION SEARCHES POST-*JONES*

*U.S. v. Graham* is one example of how lower courts have dealt with the gap between what society might consider a reasonable expectation of privacy and the uses of technology.[74] In that case, a district court in Maryland decided whether a defendant's Fourth Amendment rights could be violated when the government obtained historical cell site location data without procuring a warrant.[75] The Court denied a motion by the defendants to suppress "historical cell cite location data" that was collected.[76] The defendants were charged with conspiring to rob and robbing several fast food restaurants. [77] The police ordered the acquisition of historical cell site locations to see if the locations of the defendant coincided with the locations of the alleged crimes.[78] The police provided the magistrate with specific and articulable facts for the order, but did not ask for a warrant for lack of probable cause.[79]

The defendants in *Graham* contended that the government's lack of a warrant while searching the defendants' historical cell site location data was a violation of their Fourth Amendment rights, even if it was done pursuant to the Stored Communications Act.[80] The

---

[68] *Id.*
[69] *Id.*
[70] The "effect" in this case referred to the defendant's property, his car.
[71] *Id.*
[72] *Id.*
[73] For in both of these cases the Court focused on a different issue to dispose of the cases, and not on the main issue of the breach of privacy through the use of technology.
[74] United States v. Graham, 846 F. Supp. 2d 384, 385 (D. Md. 2012).
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.* at 387.

defendants argued that the acquisition of the historical cell site location data intruded on their expectation of privacy and therefore was an unconstitutional search because of the magnitude of the monitoring and the prolonged length of time of the investigation.[81] The argument claimed that the intrusion of their privacy was far reaching and unconstitutional due to the type of technology because the historical cell site location data allowed the government to retroactively monitor a suspect through his cellular telephone.[82] Cell phones, they said, are an integral gadget that is commonly carried by individuals at all time, including in constitutionally protected areas like homes and religious places.[83]

The state argued that the defendants had no Fourth Amendment expectation of privacy because the state considered that the historical cell site location data should have been treated as a business record that the defendants had voluntarily provided to the cell phone company.[84] The state also argued that the site location data was similar to a pen register of dialed telephone numbers and bank records disclosed to banks, which the Court had found did not implicate the Fourth Amendment.[85]

By comparing several factors to the decision in *Jones*, the court concluded that the defendants in *Graham* did not have any legitimate expectation of privacy in the "historical cell site location" records acquired by the government.[86] In that case, the court stated that according to the Fourth Amendment a government surveillance did not become a "search" only after some specified amount of time.[87] The court also made a clear distinction between GPS signals and historical cell site location data. The court stated that "historical cell site location data", was only as its name implied, the historical information that was revealed by the data, therefore, that data would only show the government where a suspect had been and not where the suspect actually was, unlike GPS which shows where a suspect is at the present time.[88] Moreover, the court stated that the cell site location data only exposed the cellular towers that were used to make a particular call.[89] Therefore, the court reasoned that the information would only disclose the overall locality of where a cellphone was being used.[90] The court also made a distinction between GPS and cell location data, asserting that the long term GPS monitoring of most investigations intruded on an individual's expectations of privacy as opposed to the temporal monitoring of when their phone was in use.[91]

Consequently, the district court concluded in *Graham* that the cellphone location records that had been used were kept in the ordinary course of business by the cellular provider, and thus were not subject to Fourth Amendment protection. Hence, the court stated that the defendants had no legitimate expectation of privacy in those records, and therefore, no Fourth Amendment violation had occurred.[92] Furthermore, the district court emphasized that it had reached its

---

[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.* at 388.
[85] *Id.*
[86] *Id.* at 389.
[87] *Id.* at 389–90.
[88] *Id.* at 391.
[89] *Id.*
[90] *Id.* at 392.
[91] *Id. at* 393.
[92] *Id.*

decision by following the Supreme Court's statement that judges should try not to rule hastily on how new technology is used, thus preventing confusion in how the use of such technology is treated, before the role of the new technology has become clear in society.[93]

Moreover, the court indicated that due to the fast changes in the dynamics of communication and information transmission in both technology and what society accepts as proper behavior, the court as prudent counsel need be cautious, and not let the facts of a case be used to establish a "far-reaching premise" for other cases with distinct sets of facts.[94] Similarly, the court in *Graham* also quoted Justice Alito's concurrence in *Jones*, which stated when the issues of a case involve dramatic technological change; the best solution would be a legislative solution. Justice Alito argued that "[a] legislative body [was] well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[95] Although this point of view seems very appropriate to conserve the integrity of the Constitution, in the long run, the variance in laws between states and the interpretations by lower courts causes more confusion, disparity, and conflict among the courts and states. Nevertheless, the circuit court in *Graham* was able to reach a solution that fit well within the decisions reached in *Miller* and *Smith,* and also balanced favorably with the *Katz* analysis.

Contrary to the decision in *Graham*, the Sixth Circuit Court of Appeals in *United States v. Skinner* decided that the use of a pay-as-you-go phone's GPS by the government without a warrant did not constitute a violation of the Fourth Amendment. [96] The fact pattern in *Skinner* was somewhat different than in *Graham*. The defendant was a "drug runner" who used a pay-as-you-go cellphone to communicate while he transported a shipment of drugs while inside the United States. The defendant presumed that the use of a pay-as-you-go cellphone was more difficult to trace.[97] However, the government used the data originating from the defendant's cellphone to determine the defendant's real-time location.[98] The State argued that the investigators collected the data from defendant while he transported the drug shipment through public roads from Arizona and Tennessee.[99] While the authorities were tracking the defendant's contact, they were able to discover the defendant's phone number which was used to communicate with his contact.[100] The authorities petitioned a federal magistrate for an order "authorizing the phone company to release subscriber information, cell site information, GPS real-time location, and "ping" data for the phone in order to learn [the defendant's] location while he was en route to deliver the drugs."[101]

The information revealed that the phone's location, allowing enforcement authorities to confront the defendant.[102] An officer approached the defendant's motor home, knocked on the door, and introduced himself to the defendant.[103] The defendant denied the officer's request to

---

93 *Id* at 404 (quoting Ontario v. Quon, 560 U.S.746, (2010)).
94 *Graham*, 846 F. Supp. 2d at 385.
95 *Id.* at 390 (quoting U.S. v Jones 132 S.Ct.945, 965 (Alito, J concurring)).
96 United States v. Skinner, 690 F.3d 772, 774 (6th Cir. 2012).
97 *Id.*
98 *Id.*
99 *Id.* at 774.
100 *Id.*
101 *Id.* at 776.
102 *Id.*
103 *Id.*

search the vehicle.[104] Subsequently, a K–9 Unit was brought to the scene; the unit conducted a routine perimeter dog sniff around the defendant's motor home.[105] The dog signaled the officers to the presence of narcotics.[106] The officers found over 1,100 pounds of marijuana in the motor home.[107] The defendant was charged with two counts related to drug trafficking and one count of conspiracy to commit money laundering.[108]

In *Skinner*, the defendant argued that the use of the GPS location information, which was produced from his phone, constituted a warrantless search that violated his Fourth Amendment right to privacy.[109] Nevertheless, the court of appeals stated that there was no Fourth Amendment violation because the defendant "[D]id not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone."[110] The court stated that the police could "certainly" use technology to track a location, using a signal emitted from a device being used by a person while transporting contraband.[111] Moreover, the Court stated that the law could not be that a criminal was entitled to depend on a perceived un-traceability of a device which he or she used while committing a crime.[112] The court indicated that advances of cellphone location technology did not change that principal. If the law allowed criminals to rely on such privacy, technology would only help criminals, not the police.[113] Furthermore, the Court stated that the cell phone's site information was constitutionally the same as the information that the government could have obtained through visual surveillance of public roads.[114] The defendant argued that, unlike *Knotts*, the DEA agents did not know the identity of the defendant, nor the type of car that was being driven; therefore, the agents would not have been able to establish any type of visual surveillance of his movements.[115] For that reason, the defendant contended that the government used technology to supplement, and "[N]ot [to] 'augment,' the 'sensory faculties' of the agents."[116] However, the court stated that when deciding whether a defendant's reasonable expectation of privacy has been violated, the court did not look at what information was known to the police, but at what the defendant had voluntarily disclosed to the public.[117] Therefore, the court reasoned that the agents could use the site information to help them locate the defendant's vehicle.[118]

In *Skinner*, the court distinguished its conclusion from the one made in *Jones*, by stating that the main issue in *Jones* was the undisclosed placement of a GPS on the defendant's vehicle.[119] Furthermore, the Court stated that in *Jones*, "[T]he Court's opinion explicitly relied

---

[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.* at 774.
[108] *Id.*
[109] *Id.* at 777.
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] *Id.* at 778.
[115] *Id.*
[116] *Id.* at 779.
[117] *Id.*
[118] *Id.*
[119] *Skinner*, 690 F.3d at 774; United States v. Jones, 132 S. Ct. 945, 948 (2012).

on the trespassory nature of the police action."[120] The court in *Skinner* then determined that, the defendant had obtained the cell phone for the purpose of personal communication, and that phone included the GPS technology that the cell phone company used to track the phone's location.[121] The court then indicated that unlike the defendant in *Jones*, the Government had never physically intruded Skinner's mobile phone.[122] Moreover, the Court in *Skinner* also differentiated by stating that in *Jones* the police had conducted intensive monitoring that expanded over a 28–day period. But that in this case, the Government agents had only tracked the defendant's mobile phone for a mere three days.[123]

Therefore, the court concluded that the monitoring was in fact a reasonably "short-term monitoring" of the defendant's movements on public roads, and that the monitoring met society's reasonable expectations of privacy.[124] The court also concluded that the use of the GPS data and the phone location did not intrude on the defendant's reasonable expectation of privacy because the Government was tracking a number that was voluntarily used while the defendant was traveling on public roads.[125]

On the other hand, Circuit Judge Donald disagreed with the majority opinion, and noted in his concurrent opinion that the defendant did not lose his expectation of privacy in the data that was given off of his mobile phone just because he used the phone during the commission of a crime.[126] Judge Donald also stated that just possessing the cellphone was not contraband *per se*.[127] Moreover, Judge Donald also disagreed with the holding of the case. According to Judge Donald, it did not matter whether the government had only used technology to locate the defendant. Judge Donald argued that the agents could not have, and indeed had not, established any visual contact with the defendant without using the phone surveillance, because the Government had not identified who the defendant was.[128] Furthermore, Judge Donald stated that the "[O]fficers could not have divined any of this information without the GPS data emitted from Skinner's phone; therefore, they [could not be] said to have merely 'augmented the sensory faculties bestowed upon them at birth.'"[129]

In *Skinner*, the Circuit Court dealt with a similar situation to the one in *Jones*, in that case Government agents conducted a search of the defendant's location through the use of technology without a warrant. However, the Court in *Skinner* narrowly followed the *Jones* decision, which ruled on the physical intrusion of government to the defendant's car, and not on whether the continuous search through the use of GPS intruded on the defendant's reasonable expectation of privacy. The Circuit Court decided the case by assimilating the facts to those in *Knotts*.

---

[120] *Skinner*, 690 F.3d at 779.

[121] In *Skinner*, the GPS signal emitted from the phone was an exact and present location similar to the GPS in *Jones*, and different from the phone data that was used in *Graham*.

[122] *Id.*

[123] *Id.*

[124] *Id.* at 780; this case differs from the previous cases because at no point did the agents actually follow the vehicle or conduct any type of visual surveillance. Moreover, the authorities did not know who the suspect was before using the GPS.

[125] *Id.*

[126] Judge Donald concurrent opinion is important as it serves as a contrasting point on the interpretation of the law, and to show the stretches of interpretation that the majority made in its decision; *Id.* at 780.

[127] *Id.*

[128] *Id.*

[129] *Id.* at 786.

However, as the defendant and Judge Donald stated, the government had not physically identified the defendant, and therefore, the agents would not have been able to follow him on public streets because they did not have an identification and did not know the type of vehicle he was driving.

It is a cause for concern that the court decided to ignore both the defendant's and society's reasonable expectations of privacy, by ignoring the importance of privacy in tracking a defendant through a cellphone—a device which people carry with them at all times. Cellphone use is unlike the physical intrusion of a car, as in *Jones*, considering that most people are not near their vehicles at all times, especially in metropolitan cities. However, some lower courts have denied the admittance of phone GPS tracking into evidence if they have not been warranted, based on their interpretation of *Jones* and the Fourth Amendment.

## VII. REASONABLENESS ELEMENT

Even when government searches would be considered unwarranted, any evidence acquired from the search may be admissible if the court finds that a warrantless exception applies. Through this method, courts are able to admit evidence with good basis and evade the conflict of the current interpretation of the Fourth Amendment and technology. One of the exceptions is the reasonableness that the government used to acquire the evidence. For instance, in *United States v. Cowan*, the Eighth Circuit Court of Appeals decided that using the alarm function of a key fob, to locate the defendant's car did not constitute a search under the Fourth Amendment.[130] There, the defendant was charged "with conspiracy knowingly to distribute cocaine base," after the defendant was arrested for possession of narcotics in his car.[131] The defendant was arrested by the police after the officers conducted a warranted search of another suspect in an apartment. During the search, the defendant was frisked and questioned about how he had arrived at the apartment.[132] The defendant responded that he had arrived through public transportation, however, one of the officers found car keys on his person during the frisk. After officers completed the warranted search the defendant was unhandcuffed.[133] The officer told him that he would be free to leave if his keys did not unlock any of the cars parked in the vicinity.[134] However, a car alarm did go off when the officer pressed the alarm key on the key fob. After the police identified the defendant's car, a police dog was used to detect drugs in the car.[135]

The defendant in *Cowan* argued that the officer's use of the key fob constituted a violation of the Fourth amendment because he had a privacy interest in the key fob's code.[136] However, the court stated that the use of the fob to locate the car was "reasonable under the forth amendment's automobile exception."[137] The court also stated that the defendant did not have a "reasonable expectation of privacy in the identity of the car."[138] Moreover, using the decision in

---

130 U.S. v. Cowan, 674 F.3d 947 (8th Cir. 2012).
131 *Id.* at 950.
132 *Id.* at 951.
133 *Id.*
134 *Id.*
135 *Id.*
136 *Id.*
137 *Id.* at 955.
138 *Id.*

*Jones*, the court concluded that the transmission of electronic signals from the fob to the car did not rise to the level of a search; especially when the defendant gave the agent permission to touch the key fob.[139]

Likewise, in *People v. Robinson*, the California Court of Appeal used the principal set forth in *Jones*, to determine whether an officer's actions constituted a search when a chattel had been trespassed.[140] In that case, the defendant was charged with: conviction of assault on a peace officer with an assault weapon, possession of heroin for sale, being a felon in possession of a firearm and ammunition, and participation in a criminal street gang.[141] The defendant argued that the use of a key to unlock his property, where the police found incriminating evidence, was a violation of the Fourth Amendment because the police did not have a warrant to enter the property.[142] Pursuant to *Cowan* and *Jones,* the defendant contended that the use of the key constituted a physical trespass on the property.[143] The Court stated that the case did advance on the theory, because the officer picked up several keys and tried to unlock the property with them.[144] Moreover, the court stated that even though there were competing authorities characterizing trespass under the common law, the testing of the key would have constituted a trespass under the common law.[145] However, the court decided that the search was not a violation of the Fourth Amendment because the search was reasonable.[146]

Likewise, the Court of Appeals held in *United States v. Lawing* that police investigators needed only a reasonable suspicion to justify the seizure of a suspect's cell phone to determine whether it was the one called by an informer to arrange a drug deal.[147] In that case, the court stated that the police did not need to secure a warrant, to identify whether the phone was used to perpetuate a drug deal. The court stated that just calling a suspect's phone did not constitute a search for Fourth Amendment purposes.[148]

## VIII. GOOD FAITH EXCEPTION

Another method that courts use to admit evidence under good basis and narrowly read into the current interpretation of the Fourth Amendment and technology is the good faith exception. In *United States v. Rosas Illescas,*[149] Immigration and Customs Enforcement agents installed a GPS without a warrant to track the movements, patterns, and to determine the identity of the individual driving the truck.[150] The agents used this information to identify the defendant.[151] After being able to confirm the identity of the subject,[152] the agents were able to

---

[139] *Id.*

[140] 145 Cal.Rptr.3d 364, 367 (2012); Although *Robinson* does not deal with search and technology, it is important to show how the Court of Appeals decided to admit evidence, which under *Jones*, would have been considered a search due to the trespassing of chattel.

[141] *Id.* at 368.

[142] *Id.*

[143] *Id.* at 373–74.

[144] *Id.*

[145] *Id.*

[146] *Id.*

[147] United States v. Lawing, 703 F.3d 229 (4th Cir. 2012).

[148] *Id.*

[149] United States v. Rosas Illescas, 872 F.Supp.2d 1320 (N.D. Ala. 2012).

[150] *Id.*

[151] *Id.*

locate him in an area he had previously frequented.[153] The court used the *Jone*s analysis to determine that the GPS installation was a search and violated the defendant's Fourth Amendment rights, but declined to exclude the evidence because it was only used to identify the defendant.[154] The court also allowed the evidence based on the good faith exception of the exclusionary rule.[155]

In *United States v. Pineda Moreno,* DEA agents used a tracking device on a mobile home on seven occasions.[156] The court determined that the DEA agents could attach the mobile trackers, based on probable cause, and also because they attached the trackers in public areas.[157]

## IX. LEGISLATIVE ALLEVIATIONS

In Florida, the interception and disclosure of wire, oral, or electronic communications is prohibited; this prohibition resembles that of the Federal Secure Communication Act. Florida Statute § 934.03 states that:

> (2)(a) 1. It is lawful under ss. 934.03-934.09 for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his or her employment while engaged in any activity which is a necessary incident to the rendition of his or her service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.
>
> 2. Notwithstanding any other law, a provider of wire, oral, or electronic communication service, or an officer, employee, or agent thereof, or landlord, custodian, or other person, may provide information, facilities, or technical assistance to a person authorized by law to intercept wire, oral, or electronic communications if such provider, or an officer, employee, or agent thereof, or landlord, custodian, or other person, has been provided with:
>
> a. A court order directing such assistance signed by the authorizing judge; or
>
> b. A certification in writing by a person specified in s. 934.09(7) that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required.

---

[152] A known alien who had previously been deported from the United States.
[153] *Id.*
[154] *Id.*
[155] *Id.*
[156] U.S. v. Pineda-Moreno, 688 F.3d 1087 (9th Cir. 2012).
[157] *Id.*

> . . . (b) It is lawful under ss. 934.03-934.09 for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his or her employment and in discharge of the monitoring responsibilities exercised by the commission in the enforcement of 47 U.S.C. ch. 5, to intercept a wire, oral, or electronic communication transmitted by radio or to disclose or use the information thereby obtained.
>
> (c) It is lawful under ss. 934.03-934.09 for an investigative or law enforcement officer or a person acting under the direction of an investigative or law enforcement officer to intercept a wire, oral, or electronic communication when such person is a party to the communication or one of the parties to the communication has given prior consent to such interception and the purpose of such interception is to obtain evidence of a criminal act.[158]

Like the state statutes, the Securities Communication Act, also aims to protect the citizens from warrantless searches. However, section 2708 of the Electronic Communications Privacy Act specifically states that "[t]he remedies and sanctions described in [chapter 2701 etq.] are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."[159] Section 2707, in turn, describes remedies for violations of the Act as including civil actions for violators other than the United States and administrative discipline against federal employees in certain circumstances.[160] Thus, violations of the Electronic Communications Privacy Act do not warrant exclusion of evidence. By including this provision, it effectively negates the exclusion of evidence that would have been collected through the violation of 18 U.S.C. S 2702. Nonetheless, the fact that government officials could request information obtained from exposure to third parties does not mean that third parties will provide the government with such information, unless the government has a warrant. Even when presented with warrants, companies may not be entirely cooperative where doing so might negatively impact their public image or relationship with their customers.

## X. SOLUTION PROPOSED

In *Jones*, the court reached an appropriate solution regarding whether the attachment of a foreign object to a person's effect constituted a search.[161] However, the Court did not resolve whether it is permissible to use technology to monitor individuals or whether such monitoring is considered a search if it invades an individual's subjective expectation of privacy, and that expectation is one society would consider reasonable. This Note proposes that when a case such as *Graham* or *Skinner* is brought to the Supreme Court on appeal, based on the expected privacy with regards to government surveillance through the use of GPS or the phone's historical cell site location data, the court should reach a decision based on *Miller* and *Smith.* In other words, this

---

[158] Fla. Stat. Ann. § 934.03 (West).

[159] 18 U.S.C. § 2708 (2013).

[160] 18 U.S.C. § 2707 (2013).

[161] An object that permitted officers to monitor the individual's location. United States v. Jones, 132 S.Ct. 945 (2012).

Note proposes that when a case presents this issue, it should be resolved by stating that the Government acquisition of data does not intrude on the individual's subjective expectation of privacy, if the individual himself has allowed the data to be collected by a third party. A ruling to this effect would help simplify the process and unify more court rulings. Even now courts try to narrowly read the Supreme Court's interpretation in an effort to permit the admission of such evidence.

The main argument against such a decision is that it would allow the government to use the information to track individuals without a warrant. It might also be argued that such a search might intrude upon an individual's expectation of privacy. Nevertheless, this sort of information is already available to third parties, who with our consent[162] are able to share the information with others.[163] Moreover, hackers or criminals might be able to access this information.[164] On the other hand, if we allow Government to access this information it will enable the government to protect us more efficiently. Likewise, the use of this type of investigation will reduce the need to expend resources tracking individuals in person.

However, this type of decision will reduce expenses in court by simplifying the rule, and establishing consistency among cases. Likewise, there will be a reduction in the amount of cases on appeal, as the interpretation of the Fourth Amendment would be clear in that regard. Another, incentive for this type of approach is that it might serve to deter criminal activity, in a similar manner that Hot Spot Policing[165] does.[166] Moreover, just because the Government would be able to legally use the data provided by third parties, it does not mean that third parties will provide the data to the Government.[167] Additionally, States will still be able to provide more security to it citizens through legislation.

## CONCLUSION

Although it is clear that the drafters of the Constitution wanted to protect people from government overreach and unreasonable searches, the government should not be prevented from using technologies that can help deter criminal activity. Likewise, it is appropriate for the government to take advantage of the same technology that criminals are using to commit crimes. Finally, although we might not want to have a complete government overreach, we ourselves are opening our privacy.

---

[162] The requisite consent may be obtained through a license of use agreement.

[163] APPLE CUSTOMER PRIVACY POLICY, http://www.apple.com/legal/warranty/privacy/ (last visited Feb. 21 2013).

[164] William M. Welch and Byron Acohido, *Reuters suspends social media editor charged with hacking*, USA TODAY (Mar. 15, 2013, 12:47 PM), HTTP://WWW.USATODAY.COM/STORY/NEWS/2013/03/14/SOCIAL-MEDIA-EDITOR-CHARGED/1988635/.

[165] Practice of engaging criminals before they commit a crime, thereby preventing crime from taking place in the first place.

[166] By people thinking they are being monitored, there is greater possibility that and individual committing crime might get caught, and therefore minimizing the possibly of them committing crimes.

[167] Third parties such as phone companies might be affected in their image, and will lose business if they are known to provide this information to the government. Likewise, the third parties might get sue themselves for providing the information.