Oklahoma Journal of Law and Technology

Volume 8 Number 1

January 2012

iRight: There's No App for That

Justin Hinderliter

Follow this and additional works at: https://digitalcommons.law.ou.edu/okjolt

Part of the Privacy Law Commons

Recommended Citation

Hinderliter, Justin (2012) "iRight: There's No App for That," *Oklahoma Journal of Law and Technology*: Vol. 8: No. 1, Article 2. Available at: https://digitalcommons.law.ou.edu/okjolt/vol8/iss1/2

This Article is brought to you for free and open access by University of Oklahoma College of Law Digital Commons. It has been accepted for inclusion in Oklahoma Journal of Law and Technology by an authorized editor of University of Oklahoma College of Law Digital Commons. For more information, please contact Law-LibraryDigitalCommons@ou.edu. 8 OKLA. J.L. & Tech. 60 (2012) www.okjolt.org

iRight: There's No App For That

© 2012 Justin Hinderliter

I. Introduction

A. The Fourth Amendment and Privacy Concerns with Technology

In modern American society, although privacy rights are undeniable, advancements in technology are inevitable. Technology's encroachment upon privacy interests and rights is on the horizon, if not underway already. In America, the history of privacy rights dates back to the Bill of Rights, specifically the Fourth Amendment's guarantee 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."¹

Privacy rights predate the founding fathers and have established roots in English legal doctrine.

As early as the 16th century, Sir Edward Coke wrote: "The house of every one is to him as his castle and fortress, as well for his defence [sic] against injury and violence as for his repose."² Thus, even before the founding fathers drafted the Fourth Amendment, privacy was a cherished and established right. Although this passage refers to the home, the Fourth Amendment, as ratified in 1791, expanded the right of privacy to persons, papers, and effects.³ Modern technological advances present novel risks of government intrusion upon personal privacy interests.

¹ U.S. CONST. amend. IV.

² Coke's Rep. 91a, 77 Eng. Rep. 194 (K.B. 1604).

³ U.S. CONST. amend. IV.

The privacy rights at issue in this comment concern not only the contexts of smartphones and tablets, but also those relating to Global Positioning Systems ("GPS"), tracking devices and other enhanced surveillance capabilities utilized by government officials. While these two areas may appear facially distinct, both share two fundamental qualities – possessory interests in property and a reasonable expectation of privacy by its user against governmental invasion. The Supreme Court has held that ownership interests include the right to be let alone from unwanted interference.⁴ Additionally, *Black's Law Dictionary* defines possessory interests as "the right to control property, including the right to exclude others." If ownership interests include the ability to exclude others, and possessory interests include the right to control property and exclude others from trespassing upon that property, and if these technological devices are considered property, then do they not deserve the same protection under the Fourth Amendment as other "effects"? If this contention is logical, and precedence is followed from previous holdings, then a person's technological property deserves this protection that is conveyed upon "effects" under the Fourth Amendment.

First, the wave of rapid technological advancement among home computers, tablet computers, laptops, and smartphones has greatly blurred the distinction between computer and cellphone. Additionally, enhanced surveillance techniques through the use of GPS tracking are greatly facilitated by the recent developments in such technology. Government officials now have the ability to monitor the movement of persons not only within public areas, but even within the private confines of their homes as well. While such innovations have produced a generally positive effect in modern society, it has come at the price of privacy. Consequently, the

⁴ Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 435 (1982). The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights.

legal system has been presented with a litany of novel and complex issues. This article focuses upon how the courts have attempted to adapt to and evaluate the continuing progression of technology in light of its potential infringement on constitutional rights.

II. Historical Background

A. Privacy Issues Involving Smartphones, GPS and Other Enhanced Surveillance

As smartphones are a relatively recent technological innovation, privacy concerns in this area have a limited history of jurisprudence. The best way to consider these devices is to assess the development of telephones, cellphones, and smartphones from one side, and the development of computers, laptops, and smartphones from the other. Smartphones blend telephone and computer technologies into a mobile, virtually autonomous device that travels on the person.

The drastic increase in technological capability has caused great difficulty in determining what constitutes a search within the meaning of the Fourth Amendment.⁵ Subsequent caselaw has questioned what is considered a search,⁶ what constitutes a "reasonable" expectation of privacy,⁷ and also evaluated novel technologies while struggling to deal with the issue of how government officials can, without a warrant, utilize new technology without violating the Fourth Amendment.⁸ With the rise of technology and its ability to gather and monitor citizens in public

⁷ Katz v. United States, 389 U.S. 347, 354 (1967). The Fourth Amendment protects the reasonable expectation to privacy for acts that are subjectively considered private. ⁸ Kyllo v. United States, 553 U.S. 27, 34 (2001).

⁵ See United States v. Garcia, 474 F. 3d 994 (2007).

⁶ Oliver v. United States, 466 U.S. 170, 179 (1984) (open field not considered curtilage); United States v. McIver, 186 F.3d 1119, 1120 (1999) (beeper attachment not considered "search"). *But see* United States v. Maynard, 615 F.3d 544, 567 (D.C. Cir. 2010) *cert. denied*, 131 S. Ct. 671 (2010), *cert. granted*, 131 S. Ct. 3064 (2011), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012) (GPS was considered a "search" because of the scope of the data collected habits of the persons, not just one point in time. Legislature has prohibited the use of this from citizens, thus society deems this as a reasonable expectation of privacy).

places and even in a person's home, the question as to what constitutes a search is still an uncertain science.⁹

Over forty years ago, in *United States v. Magana*, the Ninth Circuit held that evidence gathered by police in a private driveway is admissible.¹⁰*Magana* allowed this gathering of evidence, without a warrant, on private property¹¹ on the grounds that the driveway was only a "semi-private" area despite being within the curtilage of Magana's home.¹² *Magana* set potentially dangerous precedent that the driveway, and thus the curtilage of a citizen's home, is only a semi-private area with a reduced expectation of privacy.¹³ The Supreme Court took what some would consider an equally dangerous step in *United States v. Knotts* by concluding that technology only acts to enhance the senses of government officials, and therefore an evaluation of whether a search occurred is not a question of type, but more aptly defined as a question of scope.¹⁴ *Knotts* provided the courts with one of the first intersections of technology and law with respect to monitoring a person's movements on public roads.¹⁵ Ultimately, *Knotts* perhaps presented one of earliest examples of technology's victory over the Fourth Amendment.¹⁶

⁹ Eventually the courts will have to answer the question presented in the argument as to what constitutes as a search in public, given the scope and breadth of the searching and tracking capabilities of new technology.

¹⁰ United States v. Magana, 512 F.2d 1169, 1171 (9th Cir. 1975).

¹¹ *Id.* at 1170.

¹² *Id.* at 1171.

¹³ *Id.* The expectation of privacy largely depends on the nature of the activities being performed and the visibility of those activities from public property. Thus, the court concluded that because Magana was openly engaged in an activity that could be seen from the street, he could not have a reasonable expectation of privacy in the driveway.

¹⁴ United States v. Knotts, 460 U.S. 276, 281 (1983).

¹⁵ *Id.* at 285. The issue decided is whether the use of a beeper to monitor the progress of defendant's car violated the Fourth Amendment rights of the defendant.

¹⁶ *Id.* No constitutional issues are raised when government agents use scientific enhancement of this sort. The reasoning is validated by the stance that a police car following defendant could have observed defendant travelling on the public highways and arriving at the location of the

The Supreme Court decided Oliver v. United States nearly a decade later, holding that open fields were not considered part of the curtilage afforded protection under the Fourth Amendment.¹⁷ In *Oliver*, agents gathered evidence by walking around a gated road, disregarding a posted "No Trespassing" sign, and entered a suspect's private land.¹⁸ The Court rested its rationale on how the open fields doctrine interacts with the Fourth Amendment and how this affects the reasonable expectation of privacy.¹⁹ In holding that no Fourth Amendment violation occurred, the majority found no significant societal interest in protecting open fields, relative to the protection one's home.²⁰ However, the *Oliver* decision did not come without contest, as Justices Marshall, Brennan and Stevens all dissented on the grounds that private land marked by the owner in a fashion prohibiting entry by others should require a warrant or probable cause and should be afforded the full protections granted by the Fourth Amendment.²¹

In United States v. Dunn, the Supreme Court set forth a four-factor test for courts to apply when determining whether curtilage is protected.²² The Court identified the four factors as: the

arrest. Thus, the court reasons that the increase in technology only broadens the scope of what police are able to do, but does not constitute a new "type" of search. ¹⁷ Oliver v. United States, 466 U.S. 170, 179 (1984).

¹⁸ Id.

¹⁹ *Id.* at 179. Open fields do not constitute a proper setting for intimate activities that the Fourth Amendment is intended to protect from unwarranted government intrusion. In addition, there is no societal interest in protecting open fields, as there is at a home, commercial building, or office. Society does not recognize an expectation of privacy in open fields as reasonable. 20 *Id*.

²¹ *Id.* at 194-95. The line of reasoning that real property is not included in the list of protected areas under the Fourth Amendment is both inconsistent with previous decisions, of which the Court did not seek to overrule. In addition, the Court's reading of the actual language of the text of the Fourth Amendment is logically flawed because the court fails to explain why curtilage cannot constitute a field. The arbitrary self-fulfilling definition of curtilage seems to be applied when beneficial in the justification of the Court's decision.

²² United States v. Dunn, 480 U.S. 294, 301 (1987). Curtilage questions should be resolved with particular reference to four factors: the proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to

proximity of the area to the home, whether the area is within an enclosure surrounding the home, the nature of the use of the area, and steps taken to protect the area from outside observation.²³ The Court also elaborated on the concept of curtilage, which originated at common law, as the area immediately surrounding the home.²⁴ The central component of his inquiry was to protect the sanctity of the person's home and ensure privacy in this area.²⁵ This four-factor test issued guidance as to how police could approach a resident's home, and was specifically applied in *California v. Ciraolo.*²⁶ In evaluating whether police taking pictures of marijuana while flying over Ciraolo's back yard in an airplane was permissible,²⁷ the Court asked the question which serves as the cornerstone of the Fourth Amendment: whether a person has a "constitutionally protected reasonable expectation of privacy."²⁸ In finding no constitutional violation despite the fact that Ciraolo erected a ten-foot fence around his yard, the Court held that Ciraolo's backyard and anything therein would be visible to passengers.³⁰

²³ *Id*.

²⁹ *Id*.

³⁰ *Id.* at 215.

which the area is put, and the steps taken by the resident to protect the area from observation by onlookers.

 $^{^{24}}$ *Id.* at 300 ("The curtilage concept originated at common law to extend to the area immediately surrounding a dwelling house the same protection under the law of burglary as was afforded the house itself.").

²⁵ *Id*.

²⁶ California v. Ciraolo, 476 U.S. 207, 212 (1986).

 $^{^{27}}$ *Id.* Aerial observation of the premises at an altitude of 1000 feet was used to determine marijuana detection.

²⁸ Id.

This analysis became known as the plain view doctrine and was later followed by the Supreme Court in *Coolidge v. New Hampshire*,³¹ but the problem herein is that at some point in time, all evidence gathered by government officials will be in plain view due to technological advancements. Thus, determining what steps were taken in order to place the evidence within plain view is the preliminary determination to make when considering whether evidence obtained is within the plain view warrant exception. Following this rationale set forth in *Coolidge v. New Hampshire*, with respect to warrantless searches of smartphones and tablets, the plain view warrant exception should apply when government officials see information contained on an electronic device without taking any additional steps. If additional steps are taken in order to place the evidence in plain view, then by definition the evidence is not in plain view.

It could reasonably be argued that government officials may see a smartphone or tablet within plain view while making a legal arrest. However, it is also reasonable to infer that beyond finding the device itself, the information contained inside is not in plain view, but rather additional steps must be taken to access the information. A warrant should then be required for the police to further examine the device. Simply put, accessing the information contained within a smartphone or tablet should require further authorization even when the device itself is in plain view. This authorization should be issued by a neutral magistrate – not at the discretion of the police. Establishing a warrant requirement to access information inside any electronic device, irrespective of whether the device is in plain view or not, benefits both law enforcement as well

³¹ Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) ("It is well established that under certain circumstances the police may seize evidence in plain view without a warrant. But it is important to note that in the vast majority of cases, any evidence seized by the police will be in plain view, at least at the moment of seizure. The problem with the 'plain view' doctrine has been in identifying the circumstances in which plain view has legal significance rather than being simply the normal concomitant of any search, legal or illegal.").

as citizens by creating a bright-line rule for government officials to follow and ensuring Fourth Amendment privacy rights are better respected.

III. Current Cases and State of the Law

A. Current State of the Law for Smartphones

In Smallwood v. State, the Florida District Court of Appeals ruled that a government official was allowed to search a phone for the call history, text messages, photos, emails and other content without a warrant.³² The police, conducting a search incident to arrest, had no reason to suspect the phone contained any evidence pertaining to the arrest itself.³³ Normally. however, a warrant exception via a search incident to lawful arrest is only valid when an officer makes an arrest and searches the areas on the person or within the person's reach for weapons that may be used to effectuate the person's escape.³⁴ The officer may also search such areas in order to prevent the concealment or destruction of evidence.³⁵ If one of these conditions is met, the warrant exception applies and generally all inculpatory evidence found may be admitted.³⁶ However, this exception to the warrant requirement does not justify general searches in other areas including rooms, furniture, and other closed areas.³⁷

³² Smallwood v. State, 61 So. 3d 448, 459 (Fla. Dist. Ct. App. 2011), review granted, 68 So. 3d 235 (Fla. 2011). ³³ *Id*.

³⁴ Chimel v. California, 395 U.S. 752, 763 (1969) ("When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction."). ³⁵ *Id*.

³⁶ *Id*.

³⁷ *Id*.

The *Smallwood* court seemed aware of precedent holding that information contained within electronic devices is distinct from information contained in an actual box.³⁸ It also was aware that this precedent it relied upon not only had the potential to already be outdated, but could also be difficult to apply to smartphone searches.³⁹ The court cited *State v. Smith*, holding that a cell phone is not a "container" and that a cell phone may never be searched under the search incident to arrest exception to the warrant requirement.⁴⁰ The reasoning was that there was a great personal privacy interest in the personal data contained within smartphones.⁴¹ In addition, the *Smith* court held the exigent circumstances doctrine was inapplicable when seeking to search cell phones because there is not a particular issue of safety for the officers and any evidence that may be destroyed can be recovered.⁴² Exigent circumstances allow for warrantless searches, but require an objectively compelling reason to do so,⁴³ which was not at issue in *Smallwood*. Still, the *Smallwood* court held that *Smith*, although on point, contravened with the United States Supreme Court precedent set forth in *United States v. Robinson*, a case validating the warrantless search under the exigent circumstances doctrine.⁴⁴ *Robinson* held that closed

³⁸ State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009).

³⁹ Smallwood v. State, 61 So. 3d 448 (Fla. Dist. Ct. App. 2011), *review granted*, 68 So. 3d 235 (Fla. 2011).

⁴⁰ Smith, 920 N.E.2d at 954.

⁴¹ *Id*.

⁴² *Id.* at 955.

⁴³ Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006) ("Warrants are generally required to search a person's home or his person unless 'the exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment.").

⁴⁴ See Smallwood, 61 So. 3d at 448 ("We are, however, constrained to affirm the denial of the motion to suppress based on article I, section 12 of the Florida Constitution, which mandates we follow United States Supreme Court precedent in the area of search and seizure. Therefore, we are bound by the Supreme Court's decision of *United States v. Robinson,* 414 U.S. 218, 234 (1973), in which the Court held containers found upon a person incident to arrest may be searched without 'additional justification.' We are not unmindful, however, of the unique qualities of a cell phone which, like a computer, may contain a large amount of sensitive

containers can be reasonably searched pursuant to a valid arrest.⁴⁵ Per the Florida Constitution, the *Smallwood* court was bound by United States Supreme Court, and subsequently found the cell phone data evidence obtained by the government officials to be admissible.⁴⁶

The *Smallwood* court opined that precedent was indeed binding, but that it was misguided and inapplicable to smartphone and tablet technologies.⁴⁷ The court admitted, however, that there is a fundamental difference between technology and closed containers.⁴⁸ As such, there should be separate test that recognizes this fundamental difference, one that more accurately affords the protections of the Fourth Amendment.⁴⁹ Both *Smallwood* and *Smith* explicitly admitted that capabilities of modern smartphones are less analogous to closed containers, and instead more properly equivalent to computers.⁵⁰

The United States Supreme Court has longstanding precedence supporting the notion that

the Fourth Amendment's right to privacy applies to government invasions not just of the home,

personal information. We, therefore, also certify a question of great public importance concerning whether the general rules announced in *Robinson*, 414 U.S. 218, regarding searches incident to arrest are applicable to information contained on a cell phone held on an arrestee's person.").

⁴⁵United States v. Robinson, 414 U.S. 218 (1973).

⁴⁶ Smallwood, 61 So. 3d at 459 ("Smith is clearly directly on point as is its reasoning that a cell phone is not a "container" pursuant to Belton. However, Smith's finding that a cell phone may never be searched under the search incident to arrest warrant requirement appears to contravene existing United States Supreme Court case law, which has never made any type of evidence found on or within the reach of an arrestee entirely off limits during such a search, not even a car. Article I, section 12 of the Florida Constitution provides the right against unreasonable search and seizure as granted under the Florida Constitution, as interpreted by the United States Supreme Court. Therefore, this court is bound by the United States Supreme Court precedent.").
⁴⁷ See id. at 448 (arguing that the court should follow the United States Supreme Court precedent in the area of search and seizure pursuant the Florida State Constitution requirement).

 $^{^{48}}_{48}$ *Id.*

 $^{^{49}}_{50}$ *Id.*

⁵⁰ Id.

but also to persons.⁵¹ In 1886, however, courts presumably did not foresee the advancement into the internet age and of modern technology. The question then becomes, assuming lower courts and subsequent Supreme Court decisions follow precedent, is following this jurisprudence a wise choice given the advancement in these types of technologies? It is questionable whether decisions made even five years ago could fully comprehend the types of technological capabilities used in modern society, much less twenty-five years into the future or more. As such, should the Supreme Court make the next decision considering the warrantless search of a smartphone or tablet one of first impression?

Modern technology now blurs what was once a routine search of a person and their belongings by adding the capability to carry virtually unlimited amounts of highly personal and private information. This information pertains to, but is not limited to financial records, political views, religious beliefs, valuable intellectual property ideas, personal pictures, personal communications and classified professional data. It is reasonable to believe that the degrees and kinds of information carried on modern smartphones and tablets falls well outside the scope or need of many routine police searches. As a result, there should be required a minimum standard of reasonable suspicion or a warrant in order for government officials to search these devices.

The rate and progression with which technology is advancing makes the distinctions in technology not only one of degree and breadth, but of fundamental differences in type of information. The amount of information traditionally carried in tangible objects has little relation

⁵¹See Boyd v. United States, 116 U.S. 617, 630 (1886) (arguing the Fourth Amendment principles "apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . . the invasion of this sacred right which underlies . . . the essence.").

to the types of data contained in rapidly evolving technological devices.⁵² In effect, smartphones and tablets are creating not only a new way to communicate, but a new type of communication altogether.⁵³ This new technological type of information is unique and not similar to the amounts and degrees of information of previous generations; thus, the applicable standard governing these new types of information should also be unique.

Given current technological capabilities, mobile devices such as smartphones and tablets contain information documenting potentially every aspect of a person's life, while both at home and away. From bank records to birthdays, social security numbers to passwords, these devices have the capability to reveal a person's most sensitive, personal and critical data. Routine searches, such as a pat down, luggage check or asking a traveler to take off their shoes, reveals minimum details about the traveler, while a search of a laptop or other electronic device may reveal a person's entire life or career.⁵⁴ Consequently, the search of a modern technological device could reveal as much, if not more, information as would a search of one's entire home. As

⁵² For example, if police find a bag of marijuana on a suspect, it is merely a bag of marijuana. If the marijuana is inspected further, no additional information can truly be obtained – a visual inspection of just the item itself is sufficient to obtain all the necessary information about the object. While it is true that the marijuana can be inspected in a laboratory to determine its chemical makeup, it is still merely marijuana. Conversely, a cell phone or computer provides a different type of information altogether. If inspected, it is still merely a computer. Even if broken down into its smaller parts like a hard drive or motherboard, no information other than that relating to the computer or cell phone itself is obtained. The information stored inside the object does not pertain to what makes a cell phone a cell phone or a computer a computer; instead, it is entirely separate, unrelated information. Additionally, the amount of information available is almost beyond comparison. This comment, as written in Microsoft Word, is approximately 100 kilobytes and 33 pages worth of text. An Apple iPhone carries up to 64 gigabytes (67,108,864 kilobytes) worth of storage. Thus, 671,088 copies of this comment totaling over 22 million pages of text could fit on a very popular cell phone. It should be noted that this is uncompressed data if compressed, such numbers could be significantly increased (all numbers are approximate). ⁵³See Joshua A. Engel, Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices, 41 U. MEM. L. REV. 233, 289 (2010).

⁵⁴See Joelle Hoffman, Reasonable Suspicion Should Be Required at a Minimum for Customs Officials to Execute a Search of a Laptop at U.S. Borders: Why U.S. v. Arnold Got It Wrong, 36 W. ST. U. L. REV. 173, 181 (2009).

the search of a person's laptop, tablet, smartphone, or other electronic equivalent is not routine and is typically unnecessary, reasonable suspicion related to the kinds of highly private information contained within the device should be a minimum requirement for allowing a search. An obvious distinction is the border exception, which allows for greater protection of the sovereign at international borders, based on the public interest of safety.⁵⁵ However, the reasoning behind requiring reasonable suspicion is still applicable to the search of smartphones and tablets within the border.⁵⁶ Simply put, the information contained therein is too sensitive to not provide a protection against arbitrary searches.

In the Ninth Circuit case of *United States v. Arnold*, the defendant argued that there is a fundamental distinction between laptops and closed containers.⁵⁷ Arnold further contended that laptops are more reasonably equated to homes and the human mind than to a restrictive closed container because of the types and amount of information contained therein.⁵⁸ Arnold's analogy of a laptop to a home is based on the notion that a laptop's capacity allows for the storage of personal documents in an amount equivalent to that stored in one's home.⁵⁹ As a result, Arnold argued that a laptop is akin to the human mind because of its ability to record ideas, e-mail, internet chats and web-surfing habits.⁶⁰ If we, as a society, have a reasonable expectation of privacy in our homes, it is inarguable that we also expect to have a reasonable expectation in our

⁶⁰ Id.

⁵⁵ United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) ("Consistently, therefore, with Congress' power to protect the Nation by stopping and examining persons entering this country, the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior. Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant."). ⁵⁶ *Id.*

⁵⁷ United States v. Arnold, 533 F.3d.1003, 1006 (9th Cir. 2008).

⁵⁸ Id.

⁵⁹ *Id*.

mind. In the sense that technology is able to record and partially analyze our thoughts and habits, it is reasonable that as a society, we expect this to be protected by our Constitution as well.

In *United States v. Villamonte-Marquez*, the dissent correctly interpreted the Fourth Amendment and noted the effect that intrusions upon individual rights have on persons and society as a whole.⁶¹ In apparent opposition to the majority, the dissent contended that Fourth Amendment rights are "not mere second-class rights but belong in the catalog of indispensable freedoms. Among deprivations of rights, none is so effective in inhibiting the public, crushing the spirit of the individual and putting terror in every heart. Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government."⁶² The threat of suspicionless, warrantless, non-routine governmental searches and seizures would have an animus, chilling effect on the public at large and violates the rights established and protected by the Fourth Amendment. In light of this, the *Smith* Court acknowledged that legitimate concerns exist regarding the effect of allowing warrantless searches of smartphones.⁶³ It noted that as modern technologies allow for high-speed internet access and are capable of storing tremendous amounts of private data, warrantless searches of such devices pose a particularly significant threat to privacy rights.⁶⁴

The constitutional right to the expectation of privacy should not be retracted or diminished with respect to the use of technologically enhanced electronic devices. As Justice Harlan emphatically stated in *Katz v. United States*, "the relevant inquiry under the Fourth

⁶¹ *Villamonte-Marquez*, 462 U.S. at 598 ("Today, for the first time in the nearly 200-year history of the Fourth Amendment, the Court approves a completely unwarranted seizure and detention of persons and an entry onto private, noncommercial premises by police officers, without any limitations whatever on the officers' discretion or any safeguards against abuse.").

⁶³ State v. Smith, 124 Ohio St. 3d 163, 168, 920 N.E.2d 949, 954 (2009).

⁶⁴ Id.

Amendment has two parts: first, whether the person had "an actual (subjective) expectation of privacy," and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable."⁶⁵ As few people openly broadcast all their phone calls, text messages, and personal information stored within their devices to the public, people have an actual expectation of privacy with these devices, as well as an expectation that society, based on the breadth or persons using these devices, is prepared to see as reasonable.

In the earlier-mentioned case of United States v. Arnold, the Ninth Circuit overturned a lower court's granting of a motion to suppress the evidence gathered during the search of Arnold's electronic content on his laptop due to a lack of reasonable suspicion – typically a necessary prerequisite for such a search.⁶⁶ In Arnold, government agents at an international border checkpoint, without reasonable suspicion, accessed two icons, opened two separate files containing photographs, and viewed other files on the laptop's hard drive that ultimately led to evidence introduced to support the government's case in chief.⁶⁷ Arnold subsequently filed a motion to suppress, arguing that the government conducted the search without reasonable suspicion and thus violated his Fourth Amendment right to privacy.⁶⁸ The Ninth Circuit was not persuaded, however, as it questionably declared that "in any event, the district court's holding that particularized suspicion is required to search a laptop, based on cases involving the search of the person, was erroneous."⁶⁹ Where the Ninth Circuit errs is by trying to evaluate a laptop and person under the same Fourth Amendment analysis. The proper analysis is to evaluate whether a laptop is an "effect" within the meaning of the Fourth Amendment. Notwithstanding the border

⁶⁵ See Engel, supra note 53, at 238.
⁶⁶ United States v. Arnold, 533 F.3d.1003, 1008 (9th Cir. 2008).

⁶⁷ *Id.* at 1005.

⁶⁸ Id.

⁶⁹ *Id.* at 1008.

exception which is applicable in *Arnold*,⁷⁰ when analyzing if a laptop is indeed an "effect," the Ninth Circuit should have considered the possessory interests in Mr. Arnold's laptop. The likely result of such an analysis would be a finding of a protected privacy right; thus, a Fourth Amendment violation warranting suppression of the information would have occurred.

In a distinguishable unpublished 2002 case, the Washington Court of Appeals opined in *State v. Washington* that although police had probable cause to seize a suspect's computer, they did not have the necessary level of suspicion to conduct a search of the computer and the computer files without a warrant.⁷¹ This increased suspicion, or a warrant from a neutral magistrate, is required in order for police to conduct a search of the computer.⁷² During the lawful arrest of Washington for suspicion of auto theft, the arresting officer was entitled to search the suspected stolen vehicle and the bag inside.⁷³ However, the search of the laptop itself was considered improper because it was conducted without a warrant and no additional evidence related to the auto theft was being sought.⁷⁴ The court thus excluded the evidence by granting Washington's motion to suppress the information obtained during the warrantless search of the computer files.⁷⁵

The important issue is that the officer had no reason to search the files of the computer because the arrest was for auto theft. The arresting officer had no reasonable articulable suspicion the laptop was evidence or contained evidence concerning the auto theft. In addition, the State was incapable of stating a valid case that the files on the laptop's hard drive presented

 $^{74}_{75}$ Id. at *3.

⁷⁰ Id.

⁷¹ State v. Washington, No. 47773-1-I, 2002 Wash. App. LEXIS 142 (Wash. Ct. App. Jan. 28, 2002).

 $^{^{72}}$ *Id.* at *3.

 $^{^{73}}_{74}$ *Id.* at *2.

⁷⁵ Id.

safety concerns for the officer. Consequently, the warrant exceptions of search incident to arrest or exigent circumstances were not established, and thus the search of the computer should have been preceded by a warrant issued upon an affidavit establishing probable cause.

Due to the sheer volume of data, as well as the highly private nature of the data stored on and accessed by smartphones and tablets, courts should establish a higher protection that requires a warrant in order to search smartphones and tablets in addition to laptops. A neutral, third-party magistrate, issuing a warrant, would be in the best position to determine whether a search of one of these devices is reasonable. If the officer were to supply the magistrate with an affidavit detailing the reasons and specifying what should be searched and why, a law enforcement search would adhere to Fourth Amendment protections of the individual while simultaneously serving the societal interest of preventing criminal activity.

B. Current State of the Law for GPS and Other Enhanced Surveillance

The use of GPS tracking devices by police introduces novel privacy concerns regarding nt only when and where the installation of the GPS device takes place, but also how long the data is transmitted and tracked. In *United States v. Pineda-Moreno*, Drug Enforcement Administration ("DEA") agents observed a group of men purchasing unusually large amounts of fertilizer at a Home Depot.⁷⁶ Based upon the expertise with narcotics, the agents recognized the fertilizer as being used in drug cultivation and proceeded to follow the men outside to a vehicle owned by Juan Pineda-Moreno.⁷⁷ This was the beginning of surveillance on Pineda-Moreno that

⁷⁶ United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010), *cert. granted, judgment vacated*, 132 S. Ct. 1533 (2012) ("The motion of petitioner for leave to proceed *in forma pauperis* and the petition for a writ of certiorari are granted. The judgment is vacated, and the case is remanded to the United States Court of Appeals for the Ninth Circuit for further consideration in light of *United States* v. *Jones*, 565 U.S. (2012).").

lasted over a four-month span, including the attachment of multiple GPS surveillance devices upon the underside of a car owned by Pineda-Moreno on seven separate occasions.⁷⁸

The GPS tracking devices were attached not only while the automobile occupied private space as it was parked within the confines of Pineda-Moreno's driveway, but also during night time hours between 4:00 and 5:00 A.M.⁷⁹ However, the driveway was open to observation from the street and was not enclosed by any fence or exclusionary device, nor were any signs posted prohibiting trespassing or entrance into the driveway.⁸⁰ Information gathered by use of the GPS tracking devices attached to Pineda-Moreno's automobile ultimately resulted in agents following and stopping the vehicle.⁸¹ The stop led to the arrest of all three men inside the vehicle, and eventually to Pineda-Moreno subsequently consenting to the search of his vehicle and home.⁸² In all, the search produced over two large garbage bags full of marijuana and led to Pineda-Moreno's conviction.⁸³

In a losing effort, Pineda-Moreno moved to suppress the contested evidence in first arguing that placing the GPS device on the vehicle violated his Fourth Amendment right to privacy.⁸⁴ He contended that the attachment of the GPS device constituted an "unreasonable

- 83 *Id.*
- ⁸⁴ Id.

⁷⁸ Id.

⁷⁹ *Id.* Additionally, the time the GPS surveillance device was attached should be noted. For example, according to Oklahoma statute, a search warrant for one's home must typically be executed during the hours of six o'clock a.m. and ten o'clock p.m. 22 OKLA. STAT. ANN. § 1230 (West 2012). While the statute also states that such restrictions do not apply for non-occupied dwellings, such as a car, it is clear from the statute that legislators recognize that there are increased expectations of privacy for one's property during certain hours. As a driveway is likely to be considered the curtilage of one's dwelling, the car within such curtilage would also be entitled to a greater expectation of privacy from search or seizure during such hours.

⁸⁰ United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010), *cert. granted, judgment vacated*, 132 S. Ct. 1533 (2012).

⁸¹ *Id*.

 $^{^{82}}_{22}$ Id. at 1214.

search" because it violated his subjective expectation of privacy, one which society considers reasonable.⁸⁵ Pineda-Moreno was also unsuccessful in arguing that time of day the actions occurred, the early morning hours in which the agents entered into the driveway, was significant because he had a reasonable expectation of privacy during those hours in the morning.⁸⁶ Lastly, Pineda-Moreno asserted that the agents' continued use of the GPS tracking device to monitor the automobile's location over a four-month period violated his Fourth Amendment rights because such devices are not typically used by the public at large for surveillance purposes, therefore violating his right to privacy.⁸⁷

In rejecting Pineda-Moreno's numerous claims, Judge O'Scannlain acknowledged that his automobile was parked within the curtilage of his home at the time the GPS tracking device in question was attached.⁸⁸ However, O'Scannlain downplayed this fact with the argument that the driveway is only a semi-private area, therefore requiring further actions from Pineda-Moreno in order to establish a reasonable expectation of privacy.⁸⁹ According to O'Scannlain, Pineda-Moreno's failure to take steps to exclude public access and prohibit the view of his property invalidated his claim to a reasonable expectation of privacy.⁹⁰

Judge O'Scannlain employed precedent established in the Ninth Circuit, *United States v. McIver*, to quickly dismiss Pineda-Moreno's claim that entering the driveway at unusual, earlymorning hours violated his reasonable expectation of privacy.⁹¹ According to *McIver*, the timing

⁸⁵ Id.

⁸⁶ *Id.* at 1215.

⁸⁷ *Id.* at 1215-16.

⁸⁸ *Id.* at 1215.

⁸⁹ *Id*. One must support that expectation by adding barriers prohibiting visibility from the street and public vantage points. Pineda-Moreno failed to add and prohibiting features. ⁹⁰ *Id*.

 $^{^{91}}$ *Id*.

of the incident has no constitutional bearing to the legitimacy of the Fourth Amendment protections.⁹² Thus, based on this reasoning it can be inferred that a person has no greater reasonable expectation of privacy late at night or in the early hours of the morning than a person would during the daytime or afternoon.

Judge O'Scannlain again uses *McIver* to support the conclusion that while the car is parked on a public street or parking lot, Pineda-Moreno cannot expect privacy and thus it cannot be considered a search.⁹³ However, an omission exists in his reasoning – the GPS tracking devices were applied to the automobile not only in public areas, but also in the driveway, the curtilage, of Pineda-Moreno's home. Nevertheless, the court dismissed the attaching of the GPS devices in public citing *McIver*.⁹⁴ The court's rationale was that there is no reasonable expectation of privacy regarding automobiles in public areas.⁹⁵ However, no reasoning is given

⁹² See United States v. McIver, 186 F.3d 1119, 1123, 1126 (1999) (time of day being held as immaterial). However, consider a relevant Oklahoma statute, 22 OKLA. STAT. ANN. § 1230 (West 2012), that specifically holds that time of search is indeed material if performed upon one's home. Curtilage is part of one's home.

⁹³ *Pineda-Moreno*, 591 F.3d at 1215.

⁹⁴ *Id.* at 1212 ("Pineda-Moreno argues that the agents violated his Fourth Amendment rights by entering his driveway between 4:00 and 5:00 a.m. and attaching the tracking devices to the underside of his Jeep. We rejected a similar argument in *United States v. McIver*, 186 F.3d 1119 (1999).").

⁹⁵ *Id.* Even assuming it was, it was parked in his driveway, which "is only a semi-private area." United States v. Magana, 512 F.2d 1169, 1171 (9th Cir.1975) ("In order to establish a reasonable expectation of privacy in [his] driveway, [Pineda-Moreno] must support that expectation by detailing the special features of the driveway itself (i.e. enclosures, barriers, lack of visibility from the street) or the nature of activities performed upon it." *Maisano v. Welcher*, 940 F.2d 499, 503 (9th Cir.1991). Pineda-Moreno offers no such evidence. To the contrary, the driveway had no gate, no "No Trespassing" signs, and no features to prevent someone standing in the street from seeing the entire driveway. Additionally, one of the investigating agents testified that "an individual going up to the house to deliver the newspaper or to visit someone would have to go through the driveway and crawled under his Jeep to retrieve a lost ball or runaway cat, Pineda-Moreno would have no grounds to complain. Thus, because Pineda-Moreno did not take steps to exclude passersby from his driveway, he cannot claim a reasonable expectation of privacy in it, regardless of whether a portion of it was located within the curtilage of his home.").

to dismiss the unreasonable search claim when the GPS tracking devices were attached while the automobile was parked in the driveway. It appears that the Court is following the Ninth Circuit decision set forth in *United States v. Magana*, holding that the driveway was not private, but rather semi-private.⁹⁶ By categorizing the driveway as semi-private, the court followed *McIver* and held that there is no reasonable expectation of privacy to automobiles parked in the public arena. Under this logic, it will presumably require that a barrier be established in order to make the driveway a private area, instead of an area that is considered "semi-private" as in *Magana*.⁹⁷ This creates a requirement for people to privatize their driveways in order to be justified in relying on that area to be afforded a reasonable expectation of privacy. Likely, this would only be applicable to persons who actually own the home and have enough resources to erect a gate, garage or alternative type of barrier.

The court also dismissed Pineda-Moreno's final argument that a search occurred whenever law enforcement used the GPS tracking device not readily available to the general public.⁹⁸ In support of this argument, the court relied on *United States v. Garcia* by contending that following a car on a public street does not constitute a search within the meaning of the Fourth Amendment.⁹⁹ The rationale behind *Garcia* is that once persons avail themselves to the public eye, they have no reasonable expectation of privacy. In doing so, the court analogizes the use of GPS and the information obtained via the GPS to the act of police following a car on a public road. Following this argument, since the police are able to physically follow and observe

⁹⁶ *Magana*, 512 F.2d at 1171.

⁹⁷ *Pineda-Moreno*, 591 F.3d at 1212.

⁹⁸ *Id.* at 1216.

⁹⁹ United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) ("Should government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search.").

the car without any technological enhancements, the GPS only enhances the scope of that ability. In effect, the opinion seems to support the contention that this is a question regarding the scope of the search, rather than the kind of search performed.

The counter to such reasoning, as raised by Pineda-Moreno and mentioned by the court in its opinion, is that unwarranted use of tracking devices as a whole constitutes a search and is thus impermissible without a warrant.¹⁰⁰ In *Garcia*, Judge Posner wrote for the Seventh Circuit and stated that in the event technology imposes mass surveillance of vehicular movements, the question would have to be addressed as to what protections, if any, the Fourth Amendment guarantees the people of this country.¹⁰¹ If permissible, the protections would clearly be substantially diminished. Mass surveillance would inevitably have a chilling effect for people in all areas of life and therefore significantly reduce one's reasonable expectation of privacy. This relates directly back to the heart of the Fourth Amendment for persons to be secure in their persons, houses, papers, and effects.¹⁰²

C. Future Application by Courts and Future Policy Considerations

The reasonable expectation of privacy may soon come with a price tag. Consider for a moment the implications of the decision conveyed by the Ninth Circuit in *Pineda-Moreno*: "Pineda-Moreno did not take steps to exclude passersby from his driveway, [thus] he cannot claim a reasonable expectation of privacy in it, regardless of whether a portion of it was located within the curtilage of his home."¹⁰³ Chief Judge Alex Kozinski openly dissented to the refusal to reconsider the case and elaborated that the ruling basically protects the people who have the

¹⁰⁰ *Pineda-Moreno*, 591 F.3d at 1217.

¹⁰¹ *Garcia*, 474 F.3d at 998.

¹⁰² U.S. CONST. amend. IV.

¹⁰³ *Pineda-Moreno*, 591 F.3d at 1215.

ability to protect the zone around their houses with electric gates, fences and booths.¹⁰⁴ Seemingly, the law favors those who are in an economic position to remove themselves from the public at large. Persons that can afford property with the luxury of self-imposed borders are the only segments of the population that can withstand the potential new price of privacy. For a number of Americans, the additional costs of encircling their homes, curtilage, and driveways with gates, fences, and booths simply is not feasible and is not in line with the original requirements of the Fourth Amendment.

In order to adequately privatize their property, it would require persons to have enough land in order to erect such barriers, something that can be extremely difficult in cramped, modern cities. Additionally, it would likely require ownership of the property, subject to various housing codes and possibly homeowner association guidelines. This is not a realistic solution. With the numerous practical considerations preventing adequate privatization, this "solution" to making one's driveway a private area would likely be possible for only a select population of Americans. If this is what the *Pineda-Moreno* court is suggesting, the better question here is not where reasonable privacy interests extend to, but how much reasonable privacy interests costs. Is buying a larger tract of real estate, then erecting a barrier excluding others really the preferred solution?

Furthermore, a legitimate question as to whether surveillance with GPS tracking on automobiles constitutes a search has become more pressing.¹⁰⁵ Some critics consider decisions allowing for GPS tracking devices to be placed on vehicles in driveways and public areas to be an outright attack on the Fourth Amendment, as well as the reasonable expectation of privacy

¹⁰⁴ Adam Cohen, *The Government Can Use GPS to Track Your Moves*, TIME.COM (Aug. 25, 2010), http://www.time.com/time/magazine/article/0,9171,2015765,00.html (last accessed May 20, 2012).

¹⁰⁵ See Garcia, 474 F. 3d 994; United States v. Jones, 132 S. Ct. 945 (2012).

that it affords.¹⁰⁶ With recent decisions like *Garcia*,¹⁰⁷ the Seventh Circuit seems willing to restrict the boundaries of the Fourth Amendment in order to justify support of law enforcement actions and allows admission of evidence produced from warrantless searches.¹⁰⁸

Perhaps mass surveillance will result since it appears technology is currently outpacing law. However, there appears to be a counterbalancing of this trend currently taking place, and perhaps the scales of justice are balancing after all.¹⁰⁹ Indeed, the Supreme Court has acknowledged that technology does come with restraints.¹¹⁰ When technology crosses the boundaries as interpreted by the United States Supreme Court,¹¹¹ then a search is considered to have occurred, and should be constricted by the rights afforded by the Fourth Amendment.¹¹²

One of the Supreme Court's most recent holding regarding government surveillance, *United States v. Jones*, was argued on November 8, 2011 and was decided January 23, 2012.¹¹³ In *Jones*, government agents attached a tracking device to a suspect's vehicle, without a warrant, and followed the vehicle's movements nonstop for a month.¹¹⁴ The issues raised in *Jones* are twofold: first, whether the attaching of the device constituted a search or seizure under the Fourth

¹⁰⁶ Comment, *Seventh Circuit Holds That GPS Tracking Is Not A Search*, 120 Harv. L. Rev. 2230, 2237 (2007).

¹⁰⁷ *Garcia*, 474 F. 3d at 998.

¹⁰⁸ Id.

¹⁰⁹ United States v. Maynard, 615 F.3d 544, 567 (D.C. Cir. 2010) *cert. denied*, 131 S. Ct. 671 (2010) and *cert. granted*, 131 S. Ct. 3064 (2011) and aff'd in part sub nom. United States v. Jones, 132 S. Ct. 945 (2012) ("Were the individual subject to unfettered governmental intrusion every time he entered his automobile, the security guaranteed by the Fourth Amendment would be seriously circumscribed.") (quoting Delaware v. Prouse, 440 U.S. 648, 662-63 (1979)). ¹¹⁰ Kyllo v. United States, 533 U.S. 27, 34 (2001). Using technology that provides information

regarding the interior of the home that could not have been obtained without physical entry into the dwelling constitutes a search, and thus assures the privacy against government extended by the Fourth Amendment.

¹¹¹ See Katz v. United States, 389 U.S. 437, 354. The Fourth Amendment protects the reasonable expectation to privacy for acts that are subjectively considered private.

¹¹² *Kyllo*, 533 U.S. at 34-35.

¹¹³ United States v. Jones, 132 S. Ct. 945, 947 (2012).

¹¹⁴ *Id* at 947.

Amendment, and, second, does the use of a tracking device to monitor the movements on public streets violate the Fourth Amendment. In determining that the police's actions did indeed constitute an unreasonable search, the Court clearly articulated that Jones' car was an "effect" per the Fourth Amendment.¹¹⁵ The court did not, however, address whether a seizure occurred. It nevertheless seems indisputable then, that a person's personal technological device would also be considered an "effect" following this logic. As a result, the same protections should be afforded smartphones and tablets as well.¹¹⁶

As a result of *Jones*, the Supreme Court has reconsidered *Pineda-Moreno*, vacating the judgment and granting certiorari.¹¹⁷ Due to this new holding and the fact that the judgment was vacated, the Supreme Court is likely to require the Ninth Circuit, whom originally decided *Pineda-Moreno*, to apply its analysis of the GPS attachment in *Jones* to *Pineda-Moreno*. If so, then the evidence seized in *Pineda-Moreno* will likely be excluded due to what will presumably be declared an unlawful search of Pineda-Moreno's property. This is a "win" for those advocating for full enforcement of the Fourth Amendment and what it stands for today as well as what it stood for at the time it was initially drafted.

Jones is also important for protecting privacy interests, not just with respect to GPS attachment onto a vehicle, but to other personal effects of individuals as well. The type of effect

¹¹⁵ *Id* at 949 ("The Fourth Amendment provides in relevant part 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." It is beyond dispute that a vehicle is an "effect" as that term is used in the Amendment. United States v. Chadwick, 433 U.S. 1, 12 (1977)).

¹¹⁶ One interesting distinction in *Jones* compared to *Pineda-Moreno* is that Jones argues the attachment of the GPS device onto his vehicle is a seizure, as well as a search. However, while the *Jones* Court reaches a disposition that the government conduct constituted a search, it is silent on if the government action constituted a seizure. The Fourth Amendment protects against both unreasonable searches and seizures, in the context of the original meaning at the time the Constitution was adopted.

¹¹⁷ Pineda-Moreno v. United States, 132 S. Ct. 1533 (2012).

is not conditioned within the Fourth Amendment; hence, the fact that the item searched is a vehicle, smartphone, or handheld technological device should have little bearing on the analysis of whether the effect is searched or not. The warrant requirement, as well as the warrant exceptions, should be equally applicable as well. Furthermore, if the effect searched does not fall within an applicable exception, then it is constitutionally protected under the Fourth Amendment. Additionally, the exceptions to the warrant requirement are typically created via statute or common law, and the legislatures should acknowledge the change in society, advancements in technology, and desire of the people in a democratic state. It is an opportune time for lawmakers to act by creating clear legislation on the issue, giving the judiciary modernized rules to apply when dealing with controversies involving technology. This would cure the problem of courts relying on outdated rules which are problematical to apply to newer technologies and the types of data they contain.

IV. Impact

A. Legal Impact

The legal impact of the removing the distinction between technological devices, such as computers and smartphones, compared to ordinary closed containers would create a bright-line rule for law enforcement to follow and would also set precedent for lower courts to apply to subsequent decisions. Considering the advancement in technology over the past decade, it will become increasingly difficult to draw adequate and consistent distinctions between smartphones and computers. With the ballooning popularity of tablet computers like the iPad, a tablet computer that runs on the same operating system as the iPhone,¹¹⁸ the potential for confusion

¹¹⁸ Jay Garmon, *The New iPad Runs the iPhone OS -- and That's the Problem*, NOTEBOOK REV. (Jan. 27, 2010), http://www.notebookreview.com/default.asp?newsID=5504&review=The+new +iPad+runs+the+iPhone+OS+and+thats+the+problem (last accessed May 17, 2012).

among courts, law enforcement officials, and the public is extremely high. Distinguishing factors do indeed exist, but the similarities are abundant. That being the case, it would be logical for courts to consider the two to be the legally analyzed as one in the same and establish precedent that governs the two identically. Doing so would allow courts to no longer rely on the container association, in error, with smartphones and would give persons actual notice as to what they can expect to remain private.

Admittedly, a bright-line distinguishing technology and closed containers would arguably achieve the same purposes for law enforcement, judicial precedent, and a person's actual notice as well. However, it would still rely on the association of closed containers and smartphones as a difference of only degree, and not of kind. This has been, and would continue to be, an incorrect analogy. The two items are distinctly different. The primary reason that smartphones and other advanced technologies are different than containers is both a difference in breadth and depth of information accessible. A closed container is limited to the dimensions of the container itself. As discussed above, there is a finite amount of data, items, and materials that can occupy the container. Conversely, technological devices both store, as well as access, data from other locations. This is the key – the information accessed from other sites can create practically an infinite amount, and kind, of data that can be accessed.¹¹⁹ Consequently, depending on the device, and the way the device is used, the information searched and seized by the government is potentially infinite for all practical purposes. In theory, this extends even beyond the home, and potentially into every aspect of a person's life. Compare this to a container, which is limited to what is inside that one, specific container. The distinction between finite versus infinite is the

¹¹⁹ This can be done through "cloud computing," where information is stored on a remote server and retrieved by a device via internet.

dispositive factor, and if the Fourth Amendment is interpreted to protect persons, not places, then this seems to be an appropriate "effect" in which to achieve that purpose.

Second, in consideration of the legal impact of permitting GPS searches, an established bright-line rule would allow both citizens and the government to understand precisely what protection, if any, the Fourth Amendment provides them with regards to GPS searches and information seizures. It would provide effective notice and allow for consistent application of the Fourth Amendment protections against unreasonable searches and seizures. Additionally, a clear rule would eliminate the jurisdictional splits in the Federal Circuit Courts and remove subjective judicial interpretations of the numerous courts.

Alternatively, these may both be questions that could be solved politically through legislative action. An act of Congress, passed into law by the president, would produce the same outcome as a judicially created bright-line rule without causing any issues related to "activist judges" or separation of powers. Regardless of whether it is the judiciary or legislature that finally acts, establishing clear guidance is absolutely necessary for coping with America's modern high-tech society.

B. Social Impact

Given the increased reliance on smartphones,¹²⁰ it can reasonably be said that a United States Supreme Court decision, either enhancing or retracting privacy rights with respect to smartphones, would directly affect a large percentage of the population. As the widespread use of technology continues to expand, the effects will only increase. A decision patently affirming Fourth Amendment privacy rights with respect to smartphones and tablets would allow people to

¹²⁰ Smartphone Popularity Increases, MARKETINGCHARTS (Nov. 24, 2010), http://www.marketingcharts.com/direct/smartphone-popularity-increases-15134 (last accessed May 17, 2012).

have a greater feeling of security in their privacy interests, at least with regards to possible government intrusion of their smartphones and tablets. Conversely, a decision restricting privacy rights with respect to smartphones and tablets would cause people to have a lessened sense of security in their property because the government may access their data without their consent. This in turn may, directly or indirectly, cause persons to use smartphones and tablets in a different, more restrictive manner. People are likely less likely to store highly sensitive, personal data in such devices if they believe it will be subject to warrantless searches by the government. As a result, an extraordinary number of law-abiding, innocent Americans may be unable to use their device in the intended fashion due to privacy concerns.

The questions concerning the constitutionality of GPS surveillance creates an equally uneasy feeling of diminished privacy rights. In *Pineda-Moreno*, the court was unanimous in affirming the United States District Court's denial of defendant's motion to suppress evidence obtained from GPS tracking devices placed on defendant's automobile while parked in public and semi-private areas.¹²¹ The social impact here seems to have different effects, including some based on socioeconomic distinctions. Wealthier persons are more likely to have the ability to construct barriers, whether that be constructing fences, buying larger parcels of land or simply utilizing garages. As a result, it appears that, at least from a practical standpoint, lower-income citizens will not always be afforded the same Fourth Amendment protections as their wealthier counterparts. If this is indeed the outcome from court decisions, animus feelings from one class towards the other could be a possible result of the litigation. It is well established throughout the history of our nation that some of the greatest upheavals and social movements were born from unequal protection of our citizens. This was exemplified in the Civil Rights Movement of the

¹²¹ United States v. Pineda-Moreno, 591 F.3d 1212, 1215 (9th Cir. 2010) cert. granted, judgment vacated, 132 S. Ct. 1533 (2012).

1960s to the current issues regarding same-sex marriage and higher education admissions discrimination. When decisions are handed down that trigger dissention between societal classes, the same feelings of inequity that triggered such movements are an inevitable result. In effect, division amongst distinct groups may lead to social unrest and political pressures, possibly leading to 14th Amendment Equal Protection issues. Thus, if the United States Supreme Court affirms *Pineda-Moreno*, a holding that will likely deny Fourth Amendment protection to many within lower classes, the resulting outcome may be similar to other historically significant equal protection issues in American history.

The ultimate legal impact is still in question, as subsequent cases have declined to follow *Pineda-Moreno*.¹²² The balance between personal freedom and autonomy compared against rights of law enforcement and government personnel has been assessed and considered in *Pineda-Moreno* and prior decisions. *Pineda-Moreno* runs in favor of securing convictions over the privacy interests of the citizen. However, each of the cases mentioned herein found that probable cause and or reasonable suspicion was present at the time of the act(s) in question. Accordingly, courts thus far have eluded the question of what happens when there is no probable cause initiating the implantation of a GPS tracking device. This question is almost certainly on the horizon, and when it arrives, what justification will courts rely on?

The holding of *Pineda-Moreno* will apply pressure on courts and law enforcement to determine the boundaries of what is considered a "search" under the definition of the Fourth Amendment. In addition, *Pineda-Moreno* glaringly seems to imply that in the near future, warrantless government searches of technological effects will encroach upon areas where many

¹²² United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) *cert. denied*, 131 S. Ct. 671 (2010), *cert. granted*, 131 S. Ct. 3064 (2011), *aff'd in part sub nom*. United States v. Jones, 132 S. Ct. 945 (2012).

citizens believe they have a reasonable expectation of privacy. These potential encroachments also apply both to one's curtilage of the home as well as to a person's vehicular movements. Permitting such actions simply cannot be allowed under the Fourth Amendment.

V. Conclusion

As Chief Judge Alex Kozinski initially pointed out, social elites can still burden the costs of privacy, but the day may be coming when expansive technological capabilities will become unlimited. Put another way, it is probable that any steps taken to ensure an individual's privacy will not be sufficient to shield that person from potential technological surveillance. When that day arises, all citizens will be forced to reconsider the value they place upon privacy and choose whether or not to fight to protect the privacy rights that are guaranteed under the Fourth Amendment. When this occurs, then perhaps the reasonable expectation of privacy will no longer be contingent upon socioeconomic factors, but will be free to all persons, regardless of their income.

Technological advancements provide great advantages in individual freedoms, autonomy, and simplify some of life's everyday burdens. Telephonic communications have progressively changed from the original telephone, which allowed persons to orally communicate from different locations, to the cordless phone, allowing persons more autonomy by increased movement around their home while communicating, to cell phones, which permitted oral communication almost anywhere in America. Through the last several years, the cell phone has developed into a device which serves as much, and perhaps even more so, for the transmission of wireless data as it does for oral communication. With the advent of the smartphone, communications have largely become a combination of oral communication, text messaging, email communication, and even video phone calls to both computers and other smartphones.

31

Personal technological advancements have also expanded from other direction. The first commonly used computer by the public was the desktop computer. From that point, computers then expanded and morphed into smaller, faster, lighter, and more mobile laptop computers. Similarly, laptops have recently evolved into tablets, which are essentially handheld computers with interactive screens that have virtually every capability of a laptop. As such, it is capable of e-mail communications, as well as video phone calls both with smartphones and other tablets and computers. It could be argued that the telephone and computer have merged into the same device, or at the very least two devices with the same capabilities.

The primary issue is that smartphones and tablets have much greater capabilities than just communications among persons. Many, if not all smartphones and tablets, have cameras and storage capacities sufficient to take and store thousands of pictures. In addition, these devices often store large amounts of data including important personal information, bank account numbers, social security numbers, names and birth dates of family members and friends, addresses, potentially privileged attorney-client or spousal communications, detailed web browsing history, personal e-mails, and other types of personal data. For all practical purposes, the cellphone and computer have essentially become one, and the Supreme Court should recognize that privacy concerns with these types of technologies are distinguished, in fact, from closed containers and finite objects and spaces. The arguments that government officials have relied upon to validate their search of phones are not sufficient to justify warrantless searches.

The rationale behind the search incident to arrest, as set forth in *Chimel v. California*,¹²³ is to protect the officer and to preserve evidence from potential destruction by allowing

¹²³ Chimel v. California, 395 U.S. 752, 762-63 (1969).

government officials to secure the area immediately surrounding the person being arrested.¹²⁴ Both concerns, the safety of the officers and preservation of evidence, can be sufficiently achieved by the confiscation of the smartphone or tablet. There is no justifiable reason that government officials need to search the smartphone or tablet itself at the time of arrest without a warrant. If upon further investigation it is determined that the smartphone, tablet, or laptop should be searched, a warrant can issue without any risk of destruction of evidence or harm to officers.

The constitutionally of unwarranted governmental use of GPS tracking devices was addressed by the United States Supreme Court in *United States v. Jones*.¹²⁵ Unfortunately, the scope of the holding was very limited; a clear, precise rule regarding unwarranted searches via technological devices remains undetermined. The issue that seems ripe for question, and one that *Jones* failed to address, is whether or not the attachment of the GPS device was a seizure. Whether or not accessing the data transmitted via the GPS device in such a situation constitutes a seizure thus remains unsettled as well. The Court was able to reach a conclusion without analyzing that point, but it is inevitable that the subject be addressed in the near future. If the Supreme Court intends to remain consistent with the concept held that ownership interests include the right to exclude others from encroaching upon and interfering with property, as technological devices are considered property, the logical conclusion would be to afford that protection to such devices under the Fourth Amendment.

¹²⁴ *Id*.

¹²⁵ United States v. Jones, 132 S. Ct. 945, 948 (2012).