Journal of Civil Rights and Economic Development

Volume 32, Winter 2018, Issue 3 Article 3

Nowhere to Run, Nowhere to Hide.* Applying the Fourth Amendment to Connected Cars in the Internet-of-Things Era

Gregory C. Brown, Jr.

NOWHERE TO RUN, NOWHERE TO HIDE:* APPLYING THE FOURTH AMENDMENT TO CONNECTED CARS IN THE INTERNET-OF-THINGS ERA

BY: GREGORY C. BROWN, JR.†

"Privacy is not an option, and it shouldn't be
the price we accept for just getting on the Internet."[1]

INTRODUCTION

Imagine that you are in the market for a new motor vehicle. Like many first-time car owners, this is your first major capital purchase. After conducting your own research and looking around the showroom at the car dealership, you have decided on your dream vehicle: a car with built-in 4G LTE Internet access.[2] Once you sign all of the required paperwork at the dealer, the new car is yours. Before you drive off the car lot, you are eager to test out the car's hi-tech features. You connect your iPhone to your car to make calls and access your text messages. Highly satisfied, you begin your drive home in your new car. For now, all is well.

Several weeks later, your best friend calls you and invites you over for dinner. You gladly accept. On your way to your friend's house, you fail to stop at a stop sign. Unfortunately, a police cruiser was stationed near the stop sign, and the police officer in

*MARTHA AND THE VANDELLAS, *Nowhere to Run*, *on* DANCE PARTY (Motown 1965).

† J.D. 2018, St. John's University School of Law. Many thanks to Prof. Elaine Chiu and Rosemary LaSala for their constructive feedback on this Note. I also thank my family for their unwavering support, especially my mother, Carol Martin Brown.

1 Gary Kovacs, *Tracking our Online Trackers,* TED (Feb. 2012), http://www.ted.com/talks/gary_kovacs_tracking_the_trackers/transcript?language=en. Gary Kovacs is the former Chief Executive Officer of AVG Technologies and Mozilla Corporation. *Id.*

2 The 4G LTE connection will allow this vehicle to stream information from the Internet directly to the vehicle and to create a Wi-Fi hotspot, which allows mobile devices (such as laptops, tablets, and smartphones) to connect to the Internet by using the vehicle's Internet connection. *See 4G LTE and Wi-Fi Hotspot*, ONSTAR, https://perma.cc/7UJ7-L9M9.

the cruiser had full view of your traffic violation. The police officer pulls you over soon after.

When the officer approaches your window, she informs you that you failed to stop at the stop sign several blocks ago. After you hand the officer your license and registration, the officer notices you are wearing a baseball cap that has a picture of a marihuana leaf. The officer then asks if you have been smoking marihuana, and you quickly answer, "No." Nonetheless, the officer orders you out of the car, places you in handcuffs, and conducts an interior search of your car. The search of the interior returns nothing, so the officer decides to use your car's touchscreen display to access your text messages and call history. The officer then finds the following text-message exchange between you and a contact named "Rott":

> You: "How much did u put in the trunk?"
>
> Rott: "850g, you'll be good for a while"
>
> You: "Got it, thanks"

Through her training and expertise, the officer knew that this text-message exchange was related to illegal drug activity. As a result, the officer searched the trunk of your vehicle. In the trunk, the officer found a small box with seventeen plastic baggies. Each baggie was tied up and contained approximately fifty grams of marihuana, with the exception of one baggie, which was opened and almost empty. With this evidence, the officer places you under arrest for criminal possession of marihuana.[3] In hindsight, maybe the 1986 Chevrolet Camaro was a better option.

With the rise of Internet-connected vehicles, situations like the scenario above will become more prevalent. The percentage of new cars equipped with Internet connectivity will rise to seventy-five percent by 2020, up from only thirteen percent in 2015.[4] These

[3] On the federal level, marihuana is considered a Schedule I controlled substance, 21 U.S.C. § 812(c)(10) (2016), and possession of marihuana is a federal crime, 21 U.S.C. § 844 (2016). On the state level, possession of marihuana above certain amounts for non-medicinal purposes is a crime. *See, e.g.*, N.Y. PENAL LAW § 221.20 (LexisNexis 2016) (stating that possession of marihuana above eight ounces is a class E felony).

[4] Leo Sun, *Connected Cars in the Next Decade: 4 Numbers Everyone Should Know*, THE MOTLEY FOOL (Mar. 6, 2006, 7:05 PM), http://www.fool.com/investing/general/2016/03/06/connected-cars-in-the-next-decade-4-numbers-everyo.aspx.

Connected Cars[5] will account for an estimated 380 million vehicles on the road by 2021.[6] Currently, many cars record speed, direction, gear settings, and brake usage.[7] In the near future, cars will be so integrated with wireless networks that they will be like giant rolling smartphones – equipped with calling systems, streaming video, cameras, and apps capable of harnessing an unprecedented trove of data that vehicles will produce about themselves and the people who drive them.[8]

A recent study by the United States Department of Justice illustrates the prevalence of vehicle stops and searches by police. In 2011, more than 21.6 million American drivers aged sixteen or older were involved in a police-initiated traffic stop, comprising about 10% of the 212.3 million American drivers aged sixteen or older.[9] About 3.5% of all stopped vehicles were then searched by police, meaning over 750,000 traffic stops resulted in vehicle searches in one year.[10]

Courts have held that a search warrant is not required for a vehicle search under certain circumstances. For example, an officer may search a vehicle without a warrant if she has probable cause to believe that the automobile contains contraband.[11]

5 Connected Cars are automobiles "that have access to the Internet and [contain] a variety of sensors, and . . . are thus able to send and receive signals, sense the physical environment around them, and interact with other vehicles or entities." Edward H. Baker et al., PWC STRATEGY &, *Connected Car Report 2016: Opportunities, Risk, and Turmoil on the Road to Autonomous Vehicles,* 10 (Robert Verikiel et al. eds., 2016), http://www.strategyand.pwc.com/media/file/Connected-car-report-2016.pdf.

6 John Greenough, *The Connected Car Report: Forecasts, Competing Technologies, and Leading Manufacturers*, BUS. INSIDER (June 10, 2016, 5:33 PM), http://www.businessinsider.com/connected-car-forecasts-top-manufacturers-leading-car-makers-2015-3.

7 Michelle V. Rafter, *Decoding What's in Your Car's Black Box*, EDMUNDS, http://www.edmunds.com/car-technology/car-black-box-recorders-capture-crash-data.html (last updated July 22, 2014).

8 *See* Baker et al., *supra* note 5, at 21 (noting that Connected Cars will soon be able to "provide insights into driving patterns, touch point preferences, digital service usage, and vehicle condition, in virtually real time."). Manufacturers can use this data for "preventive and predictive [car] maintenance, optimized marketing, upselling, and *making data available to third parties*." *Id*. (emphasis added).

9 Lynn Langton & Matthew Durose, U.S. DEP'T OF JUSTICE, *Police Behavior During Traffic and Street Stops, 2011*, 3 (Sept. 24, 2013), http://www.bjs.gov/content/pub/pdf/pbtss11.pdf (stating that "[a]bout 10% of the 212.3 million U.S. drivers age 16 or older were stopped while operating a motor vehicle during their most recent contact with police.").

10 *See id.* at 9.

11 Carroll v. United States, 267 U.S. 132, 155-56 (1925). "Contraband" is defined, *infra* note 75.

However, this automobile exception has traditionally been limited to the finite space of the physical vehicle itself, such as the trunk[12] and glove compartment.[13] Since the digital data on a Connected Car may not be located in the physical car itself, there is a new legal question in applying the Fourth Amendment to Connected Cars;[14] specifically, whether a warrantless search of the physical areas of the Car also permits a search of the digital data in the Car. This Note will answer this question.

Although this Note will focus on Connected Cars, this Note is a case study symbolic of the Fourth Amendment's application to developing technology. The Supreme Court recently applied Fourth Amendment doctrine to a global positioning system (hereinafter "GPS")[15] and a cell phone.[16] These devices, along with Connected Cars, are some of the many new devices in the Internet of Things (hereinafter "IoT") that can connect to the Internet and collect and share a wide variety of data.[17] The concept of IoT goes beyond computers, smartphones, and tablets; items that were traditionally non-electronic are now being equipped with microchips and various sensors to make the devices more effective and user-friendly.[18] For example, wearable health and fitness sensors can "track and wirelessly transmit information such as heart rate, brain activity, body temperature, and hydration level"

12 United States v. Ross, 456 U.S. 798, 800 (1982) (holding that a warrantless search of containers in the trunk of a car is permissible).

13 New York v. Belton, 453 U.S. 454, 460 (1981) (holding that a police officer, incident to arrest, may search the glove compartment of the occupant's car).

14 *See* Andrew G. Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 853 (2016) (stating that "[i]f an effect is defined as the physical object, plus the digital information located in the device and the communication signals to a third-party network, then a whole new Fourth Amendment threshold has been created without clear boundaries.").

15 United States v. Jones, 565 U.S. 400 (2012). *Jones* is discussed further in Part II-C *infra*.

16 Riley v. California, 134 S. Ct. 2473 (2014). *Riley* is discussed further in Part II-C *infra*.

17 *See* Ferguson, *supra* note 14, at 812 ("As a general matter, the concept behind the Internet of Things is quite simple: objects embedded with identifiers or recognizable by sensors will be able to communicate digital information to sensors seeking to collect the information."); *See* Antigone Peyton, *A Litigator's Guide to the Internet of Things*, 22 RICH. J.L. & TECH. 9 (2016).

18 *See* Ferguson, *supra* note 14, at 812, 816; Melanie Swan, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, 1 J. SENSOR & ACTUATOR NETWORKS 217, 218 (2012).

in real time.[19] Similarly, sensors in homes can control, among other things, the temperature, the amount of light in a room, and the opening and closing of doors.[20] There are even smart refrigerators that can detect when it is running low on milk and reorder more online.[21] Since IoT technology is still in its infancy,[22] courts have not had the opportunity to apply the Fourth Amendment to these new technologies, including Connected Cars.

As IoT technology continues to evolve, Fourth Amendment protections also need to evolve in order to maintain the balance of power between individuals and law enforcement.[23] Criminal investigations are more sophisticated due to advances in technology.[24] If these investigation techniques are left unchecked, individual Fourth Amendment protections will become less effective over time.[25] To maintain the level of Fourth Amendment protection intended by the Framers of the Constitution, courts need to respond with legal rules that will protect the balance of power between individuals and law enforcement.[26] These legal rules do not expand Fourth Amendment protections beyond their intended scope; these protections only serve to maintain the constitutionally mandated balance of police power.[27]

This Note advocates that the United States Supreme Court impose a search warrant requirement for the digital data on a

19 Ferguson, *supra* note 14, at 817 n.75.

20 *Id.* at 817.

21 Peter McOwan & Louis McCallum, *When Fridges Attack: The New Ethics of the Internet of Things*, THE GUARDIAN: SCI. BLOG NETWORK (Sept. 8, 2014, 2:00 AM), http://www.theguardian.com/science/alexs-adventures-in-numberland/2014/sep/08/when-fridges-attack-the-new-ethics-of-the-internet-of-things.

22 *Id*.

23 *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 527 (2011) (describing equilibrium-adjustment theory as a "mechanism by which the Fourth Amendment maintains balance over time").

24 *See id*.; Michael Casey, *Police Radars That Can See Through Walls Worry Privacy Advocates*, CBS NEWS (Jan. 20, 2015, 4:43 PM), http://www.cbsnews.com/news/police-radars-range-r-that-can-see-through-walls-worry-privacy-advocates/ (describing a new law enforcement device that can "see through most building materials up to 12 inches thick and can detect a person's breathing from 50 feet away").

25 *See* Kerr, *supra* note 23, at 527 (opining that "if a new technology permits the government to access information that it previously could not access without a warrant, using techniques not regulated under preexisting rules that predate that technology, the effect will be that the Fourth Amendment matters less and less over time").

26 *Id.* at 482.

27 *See id.* at 527.

Connected Car.[28] For purposes of police searches, the Court should bifurcate the physical areas and the digital data on Connected Cars. This bifurcation will properly account for the greater individual privacy interests implicated in a search of digital information, as detailed in the Supreme Court decision *Riley v. California*,[29] where the Supreme Court held that police are required to obtain a warrant prior to searching digital data on a cell phone.[30] The massive trove of data located on a Connected Car is virtually similar, if not greater, to that of a cell phone.[31] Consequently, the Court's rationales in *Riley* should be extended to these Cars in order to maintain the balance of power between individuals and law enforcement.

Part I of this Note will briefly discuss the key components of a Connected Car, identify who collects the data from the Car, and examine the various uses for the data. Part I also explores whether Car owners consent to the collection of their Car's data. Part II-A will trace the historical development of the automobile exception to the Fourth Amendment, which generally permits law-enforcement officers to conduct a warrantless search of a vehicle. Part II-B will discuss how the Supreme Court has applied the Fourth Amendment to pre-Internet technologies. Part II-C will discuss two recent Fourth Amendment Supreme Court cases, *United States v. Jones*[32] and *Riley v. California*, that involve a Global Positioning System (GPS) tracking device and a cell phone, respectively. Part III-A recommends that a warrant be required for the search of digital data on a Connected Car, which serves to protect the Car owner's individual privacy interests. Part III-B addresses possible concerns about the efficacy and practicality of a warrant requirement. This Note concludes in Part IV.

[28] Remarkably, a New York Assistant District Attorney, who wished to remain anonymous, agreed that a warrant should be obtained before searching digital data on a Connected Car. Telephone Interview with Assistant District Attorney, New York (Feb. 16, 2017).

[29] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[30] *Id.* at 2495.

[31] Edward J. Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, U.S. SENATOR ED MARKEY OF MASS., at 8 (Feb. 9, 2015), https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

[32] United States v. Jones, 565 U.S. 400, 402-04 (2012).

I. WHAT IS A CONNECTED CAR?

Connected Cars will provide manufacturers with a level of insight into their customers that they have never had before.[33] Connected Cars contain several categories of data collection.[34] First, the Car records geographic location in several ways.[35] Navigation systems in the Car record the Car's physical location, the last location where the Car was parked, and "previous destinations entered into [the] navigation system."[36] Second, the Car records operational data, including vehicle speed, travel direction, and times and distances traveled.[37] Finally, the Car records various miscellaneous events, including potential crash events (sudden changes in speed), seat belt use, and air bag deployment.[38] All of this data is stored locally on the Car or transmitted to the manufacturer.[39]

Aside from data collection, cell phone integration allows certain data on the cell phone to be accessed through the Car's head unit.[40] Apple CarPlay[41] and Android Auto[42] are two examples of head-unit software that allow this cell phone connectivity. While the user only has access to certain cell phone information through the

33 *See* Baker et al., *supra* note 5, at 21 (noting that "[t]he auto industry has not had the frequent digital touch points to be able to" use the data collected from customers).

34 Markey, *supra* note 31, at 8; *see also* Andreas Habeck et al., *Connected Car, Automotive Value Chain Unbound*, MCKINSEY & COMPANY, at 47 (Sept. 2014), http://www.sas.com/images/landingpage/docs/3_McKinsey_John_Newman_Connected_Car_Report.pdf.

35 Markey, *supra* note 31, at 8.

36 *Id.*

37 *Id.*

38 *Id.*

39 *Id.* at 10. Local storage is done on a special hard drive, and a typical hard drive can hold between 100 gigabytes and 320 gigabytes of data. *See, e.g.*, *MQ01AAD***C Series*, TOSHIBA, http://toshiba.semicon-storage.com/ap-en/product/storage-products/specialty/mq01aadxxxc.html (hereinafter "Toshiba").

40 *See* Habeck et al., *supra* note 34, at 47. A head unit is "[t]he central control unit for a vehicles entertainment system." *Alphabetical Glossary of Automotive Terms*, EDMUNDS, https://www.edmunds.com/glossary/.

41 Available on select cars, Apple CarPlay allows iPhone users to access certain features on their iPhone while driving. CarPlay users can, among other things, "get directions, make calls, send and receive [text] messages, and listen to music" by using a touchscreen display, buttons on a car's display, or buttons on their steering wheel. *iOS - CarPlay*, APPLE, http://www.apple.com/ios/carplay/.

42 Android Auto is the corollary to Apple CarPlay for Android smartphones. *See Android Auto*, ANDROID, https://www.android.com/auto/.

head-unit software,[43] the Car itself has access to much more.[44] For example, Apple CarPlay "can predict where you most likely want to go using *addresses from your email, texts, contacts, and calendars*."[45] Consider this scenario: You send a text message to your friend, Jane Doe, to meet you at Utopia Pizzeria. You then decide to drive your Connected Car, with Apple CarPlay, to Utopia Pizzeria. When you connect your cell phone to your Car, the navigation system immediately suggests Utopia Pizzeria as your next destination. Assuming you have never been to Utopia Pizzeria, the Car would not know that you want to visit Utopia Pizzeria if it did not have access to your text message to Jane Doe.

The requisite privacy statements for Connected Car services detail the collection and sharing of the Car data. For example, OnStar – a multi-purpose Connected Car system with more than seven million subscribers in North America and China[46]– remotely collects and stores the Car data mentioned earlier.[47] Under the terms of OnStar's privacy statement, OnStar may use the Car's data "for any purpose,"[48] so long as they anonymize it to no longer reasonably identify the Car's owner or the Car itself; this permits OnStar to share the Car data with marketing companies and other third parties.[49]

Under certain circumstances, the privacy statements permit data to be shared with law enforcement. To retrieve data from OnStar that is traceable to a specific vehicle, police would need to obtain a warrant, subpoena, or court order.[50] OnStar and other similar systems have already received requests for this data from law enforcement.[51] These requests predate the development of

43 *See iOS - CarPlay*, *supra* note 41.

44 *See id.*

45 *Id.* (emphasis added).

46 Stefan Cross, *OnStar Tops 1 Billion Customer Interactions*, BUICK (July 29, 2015), http://media.buick.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2015/jul/0729_onstar.html.

47 *Privacy Statement*, ONSTAR, https://www.onstar.com/us/en/footer-links/privacy-policy.html; *see also* Markey, *supra* note 31, at 10.

48 *See Privacy Statement*, *supra* note 47.

49 *Id.*

50 *Id.* OnStar refuses to release the number of tracking requests they receive from police. *See* Thomas Fox-Brewster, *Cartapping: How Feds Have Spied On Connected Cars For 15 Years*, FORBES (Jan. 15, 2017, 1:10 PM), http://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/.

51 Fox-Brewster, *supra* note 50.

Connected Car systems, but they center around the same legal issues. For example, in 2009, Louisiana police obtained a warrant to compel OnStar to track a vehicle travelling from Texas to Louisiana.[52] OnStar complied, and the police found ecstasy, cocaine, and a gun inside the vehicle.[53] Moreover, if an OnStar subscriber cancels their service, OnStar will continue to collect the Car's data unless the Car owner specifically opts out of the data collection.[54]

Consumers grant manufacturers the permission to access and collect this data through their agreements to the manufacturer's privacy statements; still, these agreements do not represent true consent.[55] If manufacturers disclose in their privacy statement that they are collecting and sharing a Car owner's data, then owners are deemed to have expressly consented to the manufacturers' policies.[56] Also, if a Car owner chooses to cease the manufacturer's data collection, they are usually prohibited from using some of the Car's valuable functionalities, such as GPS.[57] To provide more transparency, some critics have advocated for an "affirmative consent"[58] principle where the Car owner would need to opt in to have certain information collected by the manufacturer.[59] Thus far, their calls have fallen on deaf ears.[60]

52 United States v. Dantzler, No. 3:10-cr-00024, 2010 U.S. Dist. LEXIS 68753, at 1 (W.D. La. June 16, 2010), *report and recommendation adopted*, No. 3:10-cr-00024, 2010 U.S. Dist. LEXIS 68483 (W.D. La. July 8, 2010).

53 *Id*. Since police obtained a warrant prior to searching the vehicle, this scenario did not pose a Fourth Amendment issue. Also, the police did not possess the car that held the data; instead they went to OnStar to get the data. Unlike this case, the scenario posed in this Note's Introduction did not involve a third party.

54 John R. Quain, *Changes to OnStar's Privacy Terms Rile Some Users*, N.Y. TIMES: WHEELS (Sept. 22, 2011, 6:00 AM), http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users/.

55 *See* Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RESEARCH CENTER (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ (stating "Some 52% of internet users believe – incorrectly – that [the company keeps confidential all the information it collects on users] and that privacy policies actually ensure the confidentiality of their personal information.").

56 *See* PAUL BERNAL, INTERNET PRIVACY RIGHTS: RIGHTS TO PROTECT AUTONOMY 36-38 (Lionel Bently et al. eds., 2014).

57 Markey, *supra* note 31, at 12.

58 *See id*.

59 *Id*.

60 *See id*.

It is important to understand that consent to the *collection* of Car data is distinct from consent to the *sharing* of the Car data with law enforcement. Car owners do not cede their Fourth Amendment rights by agreeing to these privacy statements. The rest of this Note deals with Fourth Amendment questions involved with Connected Cars.

II. FOURTH AMENDMENT JURISPRUDENCE

The Fourth Amendment provides 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.[61]

A "search" occurs when a law-enforcement officer examines a person's body, property, or another area that the person would reasonably expect to consider private "for the purpose of finding evidence of a crime."[62] A warrantless search conducted by a law-enforcement officer is per se unreasonable,[63] but the Supreme Court has carved out several exceptions to this rule that do not require a warrant prior to a search.[64] One of these exceptions is the automobile exception.

Part II-A will trace the historical development of the automobile exception to the Fourth Amendment, which generally permits law-

61 U.S. CONST. amend. IV.

62 *Search*, BLACK'S LAW DICTIONARY (10th ed. 2014); *see* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

63 Katz v. United States, 389 U.S. 347, 357 (1967). In *Katz*, the Court noted that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment…" In general, evidence obtained by law-enforcement officers as a result of an unreasonable search will be suppressed. *See* Mapp v. Ohio, 367 U.S. 643, 654-55 (1961).

64 *See, e.g.*, Carroll v. United States, 267 U.S. 132, 153 (1925) (discussing the automobile exception); Benjamin Holley, *Digitizing the Fourth Amendment: Limiting the Private Search Exception in Computer Investigations*, 96 VA. L. REV. 677, 677-78 (2010) (discussing the private search exception, which permits government agents, without a warrant, to recreate the search done by the private party so long as they do not exceed the scope of the private search). For more discussion about the exceptions to the warrant requirement, *see* Akhil R. Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994).

enforcement officers to conduct a warrantless search of a vehicle. Part II-B will discuss how the Supreme Court has applied the Fourth Amendment to pre-Internet technologies. Part II-C will discuss two recent Fourth Amendment Supreme Court cases, *United States v. Jones*[65] and *Riley v. California*,[66] that involve a Global Positioning System (GPS) tracking device and a cell phone, respectively.

A. Lesser Expectation of Privacy in Vehicles

The IoT encompasses many devices. For Connected Cars, the Supreme Court has already developed particular rules concerning the Fourth Amendment. If a law-enforcement officer has probable cause to believe that a vehicle contains contraband, he or she has the constitutional authority to search it immediately; a warrant is not required for the search.[67]

Since 1925, the Supreme Court has subjected vehicles to lesser Fourth Amendment protection because of their inherent mobility and their ability to be used for transportation;[68] the lesser expectation of privacy in vehicles is the reason why warrantless searches of vehicles are permissible. This automobile exception was first set forth in the landmark Supreme Court case, *Carroll v. United States*.[69] There, law-enforcement officers suspected that the defendants were transporting illegal goods in their vehicle.[70] As a result, the officers pulled over the defendants, searched their car without a warrant, and found illegal goods hidden underneath the seat cushions.[71] *Carroll* distinguished a vehicle search from a search of a building because "the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought;"[72] as a result, taking the time to secure a warrant may be

65 565 U.S. 400 (2012).

66 134 S.Ct. 2473 (2014)

67 Carroll v. United States, 267 U.S. 132, 156 (1925).

68 California v. Carney, 471 U.S. 386, 393-94 (1985). Under the automobile exception, the term "vehicle" includes airplanes, boats, and, under certain circumstances, mobile homes. *See, e.g.*, *id.* (motor homes); United States v. Bellina, 665 F.2d 1335, 1341 (4th Cir. 1981) (airplanes); United States v. Miller, 589 F.2d 1117, 1125 (1st Cir. 1978) (boats).

69 267 U.S. 132, 153 (1925).

70 *Id.* at 153.

71 *Id.* at 136.

72 *Id.* at 153.

impracticable.[73] The Court held that the warrantless search of a vehicle did not violate the Fourth Amendment,[74] and the Court established that concealed contraband[75] goods located within a vehicle were not subject to Fourth Amendment protection.[76]

Carroll's automobile exception was later applied to vehicles that were moved by police from the site of the stop. In *Chambers v. Maroney*,[77] police officers stopped a vehicle that matched the description of the getaway vehicle used in a gas-station robbery.[78] Both occupants were arrested, and the officers took the car to the police station to search it.[79] The warrantless search at the police station returned two .38-caliber revolvers and numerous items that belonged to the robbery victim.[80] The court held that probable cause existed to conduct the warrantless vehicle search at the police station, despite no risk that the vehicle would move out of police jurisdiction during the time it would take to secure a warrant.[81] The court also found that the officers would still have probable cause to believe that the robbery vehicle contained contraband and, thus, did not need a warrant regardless of the time lapse between the original vehicle stop and the vehicle search.[82] As long as probable cause exists, an officer is permitted to either conduct an immediate warrantless search of the vehicle, or even search the vehicle at a later time by seizing it and "presenting the probable cause issue to a magistrate."[83] Early on,

73 *Id.* at 153.

74 *Id.* at 156.

75 In this Note, "contraband" is defined as any item, prohibited by statute, that is subject to seizure and forfeiture by a designated governmental actor. *See, e.g.*, *id.* at 149-53.

76 *Id.* at 155.

77 399 U.S. 42, 44 (1970).

78 *Id.* at 44.

79 *Id.*

80 *Id.*

81 *Id.* at 52.

82 *Id.* at 48, 52. Officer safety may have also played a role in the Court's decision. *See id.* at 52 n.10 (noting that "[i]t was not unreasonable in this case to take the car to the station house. All occupants in the car were arrested in a dark parking lot in the middle of the night. A careful search at that point was impractical and perhaps not safe for the officers.").

83 *Id.*

then, the Court did not delineate an outer temporal border for the automobile exception.[84]

The Court later placed limitations on the automobile exception in *Coolidge v. New Hampshire*.[85] In *Coolidge*, the defendant was questioned by the police at his house in connection with a murder.[86] Three weeks after the initial police visit and after the police: (1) conducted a lie detector test on the defendant, (2) visited the defendant's house a second time, and (3) collected other evidence from the defendant's wife, the defendant was arrested at his house.[87] The police then searched the defendant's vehicle, which was located in the driveway adjacent to his house, and found evidence linking the defendant to the murder.[88] Still, plurality rejected the State's use of the automobile exception to justify the search of the defendant's vehicle.[89] Although the police had probable cause to search the defendant's vehicle, the plurality found that it was not impracticable to obtain a search warrant; in fact, they had "ample opportunity"[90] to do so. Distinguishing *Carroll* and *Chambers*, the plurality emphasized that the items in the defendant's car were not contraband[91] and that the opportunity to search the defendant's vehicle was not "fleeting."[92] As a result, "the application of the *Carroll* case to [*Coolidge*'s] facts would extend it far beyond its original rationale."[93] With this

84 *See id.* at 51 (noting that the warrantless vehicle search "must be made immediately without a warrant or the car itself must be seized and held without a warrant *for whatever period is necessary to obtain a warrant for the search*") (emphasis added).

85 403 U.S. 443, 461 (1971) (plurality opinion), *abrogated on other grounds by* Horton v. California, 496 U.S. 128 (1990).

86 *Coolidge*, 403 U.S. at 445.

87 *Id.* at 446-47. The second police visit to the defendant's home was done by a different pair of officers, and they were unaware of the first visit made by the other officers. *Id.* at 446.

88 *Id.* at 447-49. The police obtained a search warrant for the defendant's vehicle, but the plurality invalidated the warrant since it was not obtained by a "neutral and detached magistrate [as] required by the Constitution." *Id.* at 449. As a result, the State sought, *inter alia*, to invoke the automobile exception. *Id.* at 458.

89 *Id.* at 462.

90 *Id.* The plurality found no evidence that would permit the use of the automobile exception. *Id.* (noting there was "no alerted criminal bent on flight, no fleeting opportunity on an open highway after a hazardous chase, no contraband or stolen goods or weapons, no confederates waiting to move the evidence, not even the inconvenience of a special police detail to guard the immobilized automobile.").

91 For the definition of "contraband," *see supra* note 75.

92 *Coolidge*, 403 U.S. at 460-62.

93 *Id.* at 458.

decision, the Court prohibited the use of the automobile exception in situations where "no exigent circumstances" existed.[94] The Court also emphasized that "[t]he word 'automobile' is not a talisman in whose presence the Fourth Amendment fades away and disappears."[95] Today, due to advances in technology that allow warrants to be obtained quicker,[96] there are more instances where police would have "ample opportunity"[97] to obtain a warrant.

Despite *Coolidge*'s limitation on the automobile exception, the Court continued to extend warrantless searches in several physical areas within a vehicle, including the glove compartment,[98] center console,[99] trunk,[100] and any containers within the interior or trunk of the car.[101] Today, advances in technology have made it even quicker to obtain search warrants.[102]

B. Reasonable Expectation of Privacy: Technology in the Pre-Internet Era

Before the Internet, automobiles were an early example of how the Supreme Court applied the Fourth Amendment to new technologies. Advances in technology have continued to create new challenges for our legal framework.[103] The Fourth

94 *See id.* at 464.

95 *Id.* at 461.

96 *See infra* Part III-B.

97 *Coolidge*, 403 U.S. at 472.

98 New York v. Belton, 453 U.S. 454, 460 (1981) (holding that police, incident to arrest, may search the glove compartment of the occupant's car). *But see* Arizona v. Gant, 556 U.S. 332, 343 (2009) (holding that police may search the glove compartment of the occupant's car "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search").

99 Under *Belton*, the center console would be subject to a warrantless search because it within the reach of the driver. *See Belton*, 453 U.S. at 460 n.4.

100 United States v. Ross, 456 U.S. 798, 824 (1982) (holding that police may search the trunk of the occupant's car if they have probable cause to believe it contains contraband).

101 *See id.* (authorizing warrantless searches of containers in the trunk of the car); *see also Belton*, 453 U.S. at 460 n.4 (authorizing warrantless searches of containers within the interior of the car).

102 For further discussion on the ease of obtaining a warrant today, *see infra* Part III-B.

103 *See* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 78-79 (2005) (opining that "[w]e are now approaching a critical set of [Fourth Amendment] issues—the effects of technology of an unparalleled sophistication on our privacy"); *see also, e.g.*, Ferguson, *supra* note 14, at 825 (arguing "The Fourth Amendment, of course, did not envision the Internet of Things. In a pre-electricity, pre-telephone era, the

Amendment protects only those areas and spaces to which the Supreme Court ascribes reasonable expectations of privacy and developing technology naturally impacts society's reasonable expectations of privacy.[104] An expectation of privacy is reasonable when an individual exhibits a subjective expectation of privacy and that expectation of privacy is one that society is prepared to accept as reasonable.[105] As the Court recognizes, the reasonable expectation of privacy continues to change as technology changes over time.[106]

Originally, in *Olmstead v. United States*,[107] technology led to a lesser expectation of privacy.[108] In this 1928 Supreme Court case, the defendant was suspected of selling illegal goods,[109] so federal officers installed wiretaps in the basement of the defendant's building.[110] The wiretaps were installed without trespassing onto the defendant's property and were used to listen to his telephone conversations.[111] Later, the officers intercepted incriminating evidence from the wiretap, and the officers arrested the defendant.[112] The Court held that the wiretap was not a search under the Fourth Amendment.[113] Relying on dicta in *Carroll*, the Court indicated that the Fourth Amendment only protects against a physical search of constitutionally protected areas: one's person, papers, home, or "tangible material effects."[114] Since telephone

idea that things (or even people) could communicate wirelessly, instantaneously, and automatically did not enter into the calculation of drafting fundamental protections."). This problem is compounded when judges are unfamiliar with the basic knowledge of how certain technology works. *See, e.g.*, Ashby Jones, *Our Tech-Savvy Supreme Court*, WALL ST. J.: L. BLOG (Apr. 19, 2010, 5:56 PM), http://blogs.wsj.com/law/2010/04/19/our-tech-savvy-supreme-court.

104 Katz v. United States, 389 U.S. 347, 360 – 61 (1967) (Harlan, J., concurring).

105 *Id.* at 361.

106 *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014) (Alito, J., concurring).

107 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

108 *See id.* at 466 (noting that electronic wiretapping is permissible since there was no "actual *physical* invasion" of the individual's Constitutionally protected areas) (emphasis added).

109 The defendant was accused of importing, possessing, and selling alcohol, which was illegal at this time. *Id.* at 455; *see also* U.S. CONST. amend. XVIII, *repealed by* U.S. CONST. amend. XXI.

110 *Olmstead*, 277 U.S. at 456-57.

111 *Id.* at 457.

112 *Id.*

113 *Id.* at 466.

114 *Id.* at 465-66 (quoting Carroll v. United States, 267 U.S. 132, 149 (1925) (noting that "[t]he Fourth Amendment is to be construed in the light of what was deemed an

conversations are intangible and not physical in nature, they were not protected under the Fourth Amendment.[115]

Justice Brandeis's dissent in *Olmstead* criticized the majority's strict reliance on the original text of the Fourth Amendment.[116] Brandeis recognized that the language of the Fourth Amendment should not be construed to apply solely to its original enacted purposes.[117] Furthermore, Brandeis had the foresight to recognize that advances in technology would provide the government with more non-physical ways to seize information, which would create even greater privacy concerns.[118] In other words, as technology continues to develop and become more sophisticated, the government's surveillance capabilities will advance beyond physical interventions, so a literal understanding of the Fourth Amendment will diminish an individual's expectation of privacy over time. As a result, a broader, non-physical understanding of the Fourth Amendment is necessary to establish a proper balance between law enforcement interests and individual interests when construing the Fourth Amendment.[119]

In line with Justice Brandeis's dissent, the Court later overruled *Olmstead* in the seminal case, *Katz v. United States*.[120] In *Katz*, the government placed a voice recording device on top of a public payphone that the defendant regularly used to conduct illegal activity over telephone conversations.[121] The defendant was later arrested, and the recorded telephone conversations were admitted into evidence.[122] The Court held that the government's use of the

unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens.")).

115 *Id.* at 466.

116 *See id.* at 472 (Brandeis, J., dissenting).

117 *Id.* at 473.

118 *See id.* at 474 (opining that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."). Brandeis's prediction ultimately proved correct. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the government's use of a thermal imaging device outside of a person's home to record heat being emitted from inside the home was a "search" under the Fourth Amendment).

119 *See* McCulloch v. Maryland, 17 U.S. 316, 407 (1819) ("[W]e must never forget, that it is a constitution we are expounding.").

120 389 U.S. 347, 353 (1967).

121 *Id.* at 348. The defendant was accused of transmitting information to facilitate gambling, in violation of 18 U.S.C. § 1084 (1994). *Id.*

122 *Id.* at 348-49. Since "there was no physical entrance into the area occupied by [the defendant]," the Ninth Circuit Court of Appeals affirmed the trial court's decision to admit

recording device was a "search" under the Fourth Amendment.[123] From the outset, the Court rejected the notion that Fourth Amendment searches only apply to physical searches of constitutionally protected areas, thereby overruling the core holding of *Olmstead*.[124] The Court emphasized that "the Fourth Amendment protects people, not places."[125] The Court went on to distinguish protected activity from activity not protected under the Fourth Amendment: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But *what he seeks to preserve as private*, even in an area accessible to the public, may be constitutionally protected."[126] Here, the defendant's use of the public telephone booth was protected activity because the defendant expected the content of his conversations to remain private.[127] Since the government's search "violated the privacy upon which [the defendant] justifiably relied while using the telephone booth," the government should have obtained a warrant to conduct this search.[128]

Justice Harlan's concurrence in *Katz* expanded on the majority's argument by proposing a two-prong test for whether a person has a "reasonable expectation of privacy."[129] The first prong asks whether, depending on the facts and circumstances, the individual exhibited a subjective expectation of privacy.[130] The second prong asks whether that expectation of privacy is one that society is prepared to accept as reasonable; this involves an objective analysis.[131] Harlan's subjective-objective standard was later adopted by the Court to determine whether a particular

the telephone conversations into evidence. Katz v. United States, 369 F.2d 130, 134 (9th Cir. 1966), *rev'd*, 389 U.S. 347 (1967).

123 *Katz*, 389 U.S. at 353.

124 *Id.*

125 *Id.* at 351.

126 *Id.* (emphasis added) (citations omitted). This distinction echoes Justice Brandeis's assertion that an individual's expectation of privacy will change along with developing technology. *See* Olmstead v. United States, 277 U.S. 438, 472-74 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

127 *See Katz*, 389 U.S. at 353.

128 *Id.*

129 *Id.* at 361 (Harlan, J., concurring).

130 *Id.*

131 *Id.*

governmental investigative technique constituted a Fourth Amendment search[132] and *Katz* continued to be the guidepost for a long time in the Fourth Amendment framework.[133]

C. Reasonable Expectation of Privacy: Technology in the Post-Internet Era

Even within this *Katz* framework, the rise of the Internet and continued development of technology have created a new host of Fourth Amendment issues.[134] The Framers did not envision devices that could instantly pinpoint one's location and contain massive troves of data, yet still be able to fit in the palm of your hand.[135] Nevertheless, the Supreme Court recently confronted the challenge of applying the Fourth Amendment to two post-Internet technologies: a GPS tracking device in *United States v. Jones* (2012) and a cell phone in *Riley v. California* (2014).[136] In these cases, the Court expounded upon the subjective-objective test for the reasonable expectation of privacy and provided more guidance on its application to these new technologies.[137]

Jones addressed whether "the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment."[138] There, the government placed a GPS tracking device underneath the defendant's car and used the GPS to monitor the vehicle's movement for twenty-eight days.[139] Despite holding that the government's installation of the GPS device was a "search" under the Fourth Amendment,[140] the Court deviated from the

132 *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 739-41 (1979) (applying the *Katz* analysis as detailed by Justice Harlan).

133 *See Katz*, 389 U.S. at 353.

134 *See* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1322 (2002).

135 *Id.*

136 United States v. Jones, 565 U.S. 400 (2012); Riley v. California, 134 S. Ct. 2473 (2014).

137 *See generally Jones*, 565 U.S. at 409; *Riley*, 134 S. Ct. at 2493.

138 *Jones*, 565 U.S. at 403.

139 *Id.* During those twenty-eight days, the GPS tracking device transmitted over 2,000 pages of data. *Id.*

140 *Id.* at 404.

"reasonable expectation of privacy" test articulated in *Katz* in favor of the traditional, property-based approach from *Olmstead*.[141] In the majority opinion, Justice Scalia emphasized the physical intrusion of the defendant's car and how the intrusion fit within the original scope of the Fourth Amendment.[142] Although Justice Scalia acknowledged that recent cases deviated from *Olmstead*'s property-based approach, Scalia insisted that *Katz* did not eliminate the *Olmstead* approach;[143] in fact, Scalia noted that the reasonable expectation of privacy test "has been added to, not substituted for,"[144] the *Olmstead* approach. Thus, after *Jones*, there is now a three-prong test used to determine whether a particular governmental investigative technique has violated the Fourth Amendment: (1) the technique must be a physical trespass upon a constitutionally protected area; (2) the trespass must be done to obtain information; and (3) the *Katz* reasonable expectation of privacy test must be satisfied.[145]

In separate concurrences in *Jones*, Justices Alito and Sotomayor both agreed that GPS tracking can reveal intricate details about a person.[146] Justice Sotomayor observed that advances in technology will generate more nonphysical modes of surveillance, which would render the trespassory test less useful, but "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis."[147] As a result, Sotomayor believed that both long-term

141 *Id.* at 405-07.

142 *Id.* at 404-05. This rationale was used to buttress the plurality's arguments in *Olmstead*, so it is difficult to argue that this is not a return to the *Olmstead* approach. *See* Olmstead v. United States, 277 U.S. 438, 465-66 (1928), *overruled by* Katz v. United States, 389 U.S. 347, 353 (1967), *and* Berger v. New York, 388 U.S. 41, 80 (1967).

143 *But see* Ferguson, *supra* note 14, at 831 n.161. Ferguson notes that the Court's "assertion belies the history and general discussion of the issue, which has long left the *Olmstead* line of cases in the graveyard of Fourth Amendment history." Scholars have questioned whether the Court's return to *Olmstead* was justified. *See, e.g.*, Erin Murphy, *Back to the Future: The Curious Case of* United States v. Jones, 10 OHIO ST. J. CRIM. L.325-26, 340 (2012); Thomas K Clancy, United States v. Jones*: Fourth Amendment Applicability in the 21st Century*, 10 OHIO ST. J. CRIM. L. 303, 322-23 (2012).

144 *Jones*, 565 U.S. at 409 (emphasis omitted).

145 *See id.* at 407-08 n.5.

146 *Compare id.* at 430 (Alito, J., concurring) *with id.* at 415 (Sotomayor, J., concurring) ("In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention.").

147 *Id.* at 415 (Sotomayor, J., concurring). This can occur when the government is given remote access to "factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones." *Id*.

and short-term GPS monitoring might impinge on reasonable expectations of privacy.[148] Similarly, Justice Alito believed that only long-term GPS monitoring may impinge on reasonable expectations of privacy, but short-term GPS monitoring probably would not.[149] Neither Sotomayor nor Alito delineated when exactly long-term GPS tracking of a vehicle would commence, but Alito found that "the line was surely crossed before the 4-week mark."[150]

Soon after *Jones*, the Supreme Court addressed the privacy interests implicated in one of the most pervasive forms of technology today—the cell phone.[151] In *Riley v. California*, the Court decided whether a warrantless search of digital data on a cell phone is permissible under the Fourth Amendment.[152] In two separate incidents, police officers recovered a cell phone following a search incident to arrest.[153] Through the normal operation of each cell phone, the officers accessed incriminating information by reviewing call records, pictures, and videos on each phone without

148 *Id.* at 417. Justice Sotomayor also discussed the third-party doctrine – the idea that an individual does not have a reasonable expectation of privacy in information voluntarily shared with third parties. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976). Sotomayor argued that the doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417. The third-party doctrine is at issue in a pending Supreme Court case – Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) – where law-enforcement officials obtained 127 days' worth of the defendant's cell phone records from their cell phone company. These records contained the location and movements of the defendant's cell phone, which was used to connect the defendant to a robbery in that area. This Note will not be eclipsed by *Carpenter*'s outcome. Unlike the scenario in this Note's introduction, the law-enforcement officials in *Carpenter* worked with the holder of the data to obtain the data. *See supra* Introduction. Also, law enforcement in *Carpenter* relied on the Stored Communications Act, which allows phone companies to share phone records when the government provides "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (2016).

149 *Jones*, 565 U.S. at 430 (Alito, J., concurring).

150 *Id.*

151 Cell-phone ownership in the United States is staggering. In 2015, more than 92% of adults owned a mobile phone of some kind, including smartphones. Among adults ages 18-29, this figure rises to 98%. *See* Monica Anderson, *Technology Device Ownership: 2015*, PEW RESEARCH CENTER (Oct. 29, 2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

152 Riley v. California, 134 S. Ct. 2473, 2480 (2014). *Riley* focuses on searches incident to arrest, but the implications of its reasoning reach far beyond this narrower issue. *See id.* at 2485. Even though *Riley* addressed the retention of the warrant requirement for cell phone searches, courts have relied on *Riley* to apply other Fourth Amendment doctrines to cell phones. *See, e.g.*, United States v. Sparks, 806 F.3d 1323, 1336 (11th Cir. 2015) (relying on *Riley* to apply the Fourth Amendment private search exception to cell phones).

153 *Id.* at 2480-81. In a consolidated opinion, both David Riley and Brima Wurie had their cell phones taken from their person. *Id.*

obtaining warrants.[154] The Court held that police officers must obtain a warrant before searching the digital information located on a cell phone.[155] In reaching its holding, the Court differentiated physical objects from digital content on a cell phone.[156] For example, to ensure officer safety, police officers may conduct a warrantless search of a suspect incident to arrest.[157] As a result, the officers could search the physical parts of a cell phone to ensure there are no concealed razor blades within.[158] However, the Court noted that cell-phone data presented no threat to officer safety.[159]

In *Riley*, the Court emphasized that a search of digital information on a cell phone implicates greater individual privacy interests than a physical search.[160] Cell phones implicate greater privacy interests due to their large storage capacity, the variety of information they can store, and the possibility that a search may extend beyond the data on the phone itself.[161] As the Court indicated, "A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a [cell] phone."[162]

The Court's emphasis on these three factors suggest that any device with similar capabilities to a cell phone would be subject to a warrant requirement.[163] The Court did not need to predict what

154 *Id.* at 2480-81. Riley had a smartphone, which has a wide range of features and large storage capacity, while Wurie had a flip phone, which generally has less features than a smartphone. *Id.* Neither cell phone was password protected. *Id.*

155 *Id.* at 2485. The Court refused to extend the "search incident to arrest" exception to cell phones, which generally allows police officers to search an arrestee in order to preserve evidence or ensure the safety of the officer. *Id.*; *see* Chimel v. California, 395 U.S. 752, 763-64 (1969).

156 *Riley*, 134 S. Ct. at 2484. By making this distinction, the Court was able to avoid adhering to the precedent in its previous "search incident to arrest" cases. *See id.* at 2484-85.

157 *See Chimel*, 395 U.S. at 764.

158 *See* United States v. Robinson, 414 U.S. 218, 234-35 (1973). In *Robinson*, the Court found that an officer could conduct a search incident to arrest because the "danger to an officer is far greater in the case of the extended exposure which follows the taking of a suspect into custody and transporting him to the police station." *Id.*

159 *Riley*, 134 S. Ct. at 2485 (stating "Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape.").

160 *Id.* at 2488-89 (noting that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse").

161 *See id.* at 2489-91.

162 *Id.* at 2489.

163 Ferguson, *supra* note 14, at 834 (noting "While Riley addressed the existing technologies of smartphones in 2014, the broader conclusions apply to any smart device

other devices may be analogized to a cell phone; however, with Connected Cars entering the marketplace, the privacy interests implicated in IoT devices must be explored.

III. SAFEGUARDING OUR PRIVACY: THE NEED FOR A WARRANT REQUIREMENT

To protect the privacy interests of Connected Car users, the Supreme Court should extend the rationales of the *Riley* case and require law enforcement officials to obtain a warrant before searching any data on a Connected Car. As previously discussed, cell phone searches implicate greater individual privacy interests.[164] Since Connected Cars share many cell-phone attributes, Connected Cars should also implicate greater individual privacy interests. In comparing a cell phone with a Connected Car, the three-prong *Jones* test is useful.

A. Jones Applied to Connected Cars

Applying the three-prong *Jones* test to a Connected Car illustrates its similarity to a cell phone.[165] First, in the Introduction scenario,[166] the police officer conducted a physical trespass on the Car. The officer conducted a physical search by searching the interior of the Car and using the head-unit touchscreen to search the electronic data on the Car. This situation appears to combine the searches conducted in *Carroll*[167] and *Riley*.[168] Assuming the officer reasonably believed there was marihuana inside the vehicle, the physical search would be

that can track, collect, share, store, and process personal data about its owner."); s*ee Riley*, 134 S. Ct. at 2489 (arguing "The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone.").

164 *See Riley*, 134 S. Ct. at 2488-89.

165 In applying the *Jones* test, consider the scenario detailed in the Introduction of this Note. *See supra* Introduction.

166 *Id.*

167 Carroll v. United States, 267 U.S. 132, 135 (1925). In *Carroll,* law-enforcement officers suspected that the defendants were transporting illegal goods in their vehicle, pulled over the car and searched it without a warrant; they found illegal goods under the seat cushions.

168 *Riley*, 134 S. Ct. at 2480-81. In *Riley*, the police officer obtained the defendants' respective cell phones and searched them.

permissible under *Carroll*.[169] Warrantless access to digital records is precisely what the *Riley* Court sought to avoid.[170]

Second, the physical trespass was done to obtain information. The officer looked for evidence of marihuana in the interior and trunk of the Car, and she looked on the Car's head unit to find any evidence of marihuana activity.

The third prong of the *Jones* test is the reasonable expectation of privacy test from *Katz*. As previously stated, the two-pronged reasonable expectation of privacy test first asks whether the individual exhibited a subjective expectation of privacy, and then whether that expectation of privacy is one that society is prepared to accept as reasonable.[171] Each of these two prongs will be addressed in turn. For the first prong, the Car driver exhibited a subjective expectation of privacy by not consenting to a search of her vehicle, which included the electronic data. In this instance, lack of consent may be the only way to prove that the driver maintained a subjective expectation of privacy in her vehicle.[172]

Applying the second prong of the reasonable expectation of privacy test, which involves an objective analysis of the analogy between a Connected Car and a cell phone, presents challenges. On one hand, the Connected Car is a vehicle, which is normally subject to a lesser expectation of privacy.[173] On the other hand, with all the data they contain and can reveal, Connected Cars hold "the privacies of life" and should implicate greater privacy interests.[174] In his concurrence in *Riley*, Justice Alito advocated for a revised balancing of law enforcement interests and privacy interests due to changes in technology,[175] and he urged Congress or state legislatures to delineate "reasonable distinctions based on categories of information or perhaps other variables."[176]

169 Marihuana is classified as a Schedule I drug under federal law, which would make it contraband. *See* 21 C.F.R. § 1308.11(d)(23) (2016); *see also supra* note 75 (defining "contraband").

170 *See Riley*, 134 S. Ct. at 2488-89.

171 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

172 *See* United States v. Jones, 565 U.S. 400, 413-14 (2012) (Sotomayor, J., concurring).

173 *See* Carroll v. United States, 267 U.S. 132, 155-56 (1925).

174 *See Riley*, 134 S. Ct. at 2495.

175 *Id.* at 2496-97 (Alito, J., concurring). Alito agreed with the majority that pre-digital precedent from previous "search incident to arrest" cases should not be mechanically applied to a cell phone search. *Id.* at 2496.

176 *Id.* at 2497.

The *Riley* majority delineated three potential variables in finding that cell phones implicate greater privacy interests: their large storage capacity, the variety of information they can store, and the possibility that a search may extend beyond the data on the phone itself.[177] These three variables are applicable to Connected Cars.

Firstly, Connected Cars have a large storage capacity. Connected Cars can store the data they collect on the Car onto a special hard drive;[178] these hard drives typically hold between 100 gigabytes and 320 gigabytes of data.[179] This is a massive amount of storage capacity. For comparison, a mere sixteen gigabytes can store "millions of pages of text, thousands of pictures, or hundreds of videos" on a cell phone.[180] Along with cell phones, Connected Car storage capacity will only continue to increase in the future.[181]

Secondly, Connected Cars store a wide variety of information. Aside from operational data, potential crash events, and other types of information detailed in Part I, Connected Cars also record geographical location through GPS tracking.[182] Connected Cars and cell phones both contain GPS tracking capabilities.[183] If a law-enforcement officer were able to search through the historical location information on the Car, the officer would be able to reconstruct the inconspicuous intimate details of the Car owner's life, which is normally far beyond the scope of any police search.[184] As Justice Sotomayor noted in *Jones*, both short-term and long-term "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[185]

177 *See id.* at 2489-91.

178 *See supra* Part I.

179 *See* Toshiba, *supra* note 39.

180 *See Riley*, 134 S. Ct. at 2489 (citing United States v. Jones, 565 U.S. 400, 413-14 (2012) (Sotomayor, J., concurring).

181 *See* Orin S. Kerr, *Privacy, Security, and Human Dignity in the Digital Age: Foreword: Accounting for Technological Change*, 36 HARV. J. L. & PUB. POL'Y 403, 404-05 (2013).

182 *See supra* Part I.

183 *See Riley*, 134 S. Ct. at 2490; Habeck et al., *supra* note 34, at 14.

184 *See* United States v. Jones, 565 U.S. 400, 415-18 (2012) (Sotomayor, J., concurring).

185 *Id.*

Thirdly, a data search on a Connected Car might extend beyond the data on the Car itself. This is especially true with cell phone integration.[186] Through Apple CarPlay and Android Auto, Car owners have direct and indirect access to the data stored on their phone.[187] In the Introduction scenario, the officer's search went beyond the data on the Car when she used the Car's head unit to access text messages and call records that were located on the cell phone.[188] Additionally, to retrieve vehicle data from a Connected Car system like OnStar, OnStar requires law enforcement officials to obtain a warrant anyway.[189] Thus, the three *Riley* variables have been satisfied, and the second prong of the reasonable expectation of privacy test has been met. As a result, Connected Cars should implicate greater privacy interests, and a warrant requirement would protect these interests.

With a warrant requirement in place for digital data on Connected Cars, the officer's warrantless search in the Introduction scenario would have ceased once the officer finished searching the interior of the Car. Aside from the three variables from *Riley*, consider the original reason for the automobile exception in *Carroll*: to find contraband.[190] In the Introduction scenario, the contraband sought by the officer was marihuana. Once the officer found nothing in the physical vehicle, the warrantless search should have ceased. Instead, the officer began to search through the Car's digital data. It cannot be argued that the officer continued to search for the contraband marihuana on the Car's head unit data, so the warrantless search should not have extended into the Car's head unit.

B. Opposing the Warrant Requirement

1. Impact on Law Enforcement

It is conceded that the warrant requirement for data on Connected Cars will impact how police officers do their jobs.[191]

186 *See supra* Part I.
187 *See id*.
188 *See supra* Introduction.
189 *See Privacy Statement*, *supra* note 47; *supra* Part I.
190 *See* Carroll v. United States, 267 U.S. 132, 155-156 (1925).
191 The *Riley* Court anticipated the same with cell phones. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014).

Cell phones can provide valuable information to help prosecute criminals.[192] A warrant requirement could also deter officers from pursuing low-level offenders. Nonetheless, individual rights cannot be sacrificed for the sake of officer convenience, so "[p]rivacy comes at a cost."[193]

To reiterate, my proposal for a warrant requirement does not prevent police officers from searching the physical vehicle under circumstances that warrant it. My purpose is to simply require officers to obtain warrants before searching digital data on a Connected Car.[194]

Under *Coolidge*, police may still justify a warrantless search of data on a Connected Car if exigent circumstances exist;[195] this could include preventing the imminent destruction of evidence and rendering emergency assistance to people who are injured or threatened with imminent injury.[196] For example, in the Introduction scenario, if the text message from Rott actually said "5 IEDs, that should do the trick," then the officer would be permitted to check the trunk in order to protect herself and those around her.

Also, several states now have judges on-call 24/7 to sign warrants.[197] Judge Dale O. Harris, a Minnesota state court judge, is one of the many judges that sign warrants outside working hours.[198] The officer would bring the completed warrant and affidavit of support to the judge's location for the judge to sign, even if it was a holiday, outside of work hours, or the judge was at his home.[199] Interestingly, Judge Harris noted that many of the warrants he currently signs involve searches of cell phones and

192 *Id.*

193 *Id.*

194 *See id.*

195 *See* Coolidge v. New Hampshire, 403 U.S. 443, 464 (1971) (plurality opinion), *abrogated on other grounds by* Horton v. California, 496 U.S. 128, 137 (1990).

196 *See* Kentucky v. King, 563 U.S. 452, 460 (2011).

197 *See, e.g.*, Dale Harris, *A Judge's View: Warrants Can't Wait, So a Judge Always is On Call*, DULUTH NEWS TRIBUNE (Jan. 6, 2016, 3:13 PM), http://www.duluthnewstribune.com/opinion/3918552-judges-view-warrants-cant-wait-so-judge-always-call; Sarah Mervosh, *Dallas County Judges On Call 24/7 to Sign Warrants*, DALLAS NEWS (Dec. 25, 2015), http://www.dallasnews.com/news/news/2015/12/25/dallas-county-judges-on-call-247-to-sign-warrants.

198 *Id.*

199 Harris, *supra* note 197.

computers.[200] According to Judge Brandon Birmingham, a state court judge in Texas, reading through the affidavit and signing the warrant only takes about fifteen minutes.[201]

Today, recent technological advances have made it easier to obtain a warrant. More than thirty states currently allow electronic warrant applications in various forms, including "telephonic or radio communication, electronic communication such as e-mail, and video conferencing."[202] For example, in one county in Kansas, "[P]olice officers can e-mail warrant requests to judges' iPads; judges have signed such warrants and e-mailed them back to officers in less than 15 minutes."[203] Federal magistrate judges can also issue warrants based on "information communicated by telephone or other reliable electronic means."[204] While this may not be a perfect solution, individual privacy interests cannot be sacrificed merely for the sake of police convenience.[205] Instead, law enforcement must work with technology to meet the strict mandates of the Constitution.[206] By discouraging law enforcement from embarking on fishing expeditions for evidence based on post-hoc rationalizations, an appropriate safeguard will be in place to protect the car-owner's privacy interests.

2. "Overprotection" for Connected Cars

Some may argue that this warrant requirement favors protection of Connected Cars over traditional automobiles. In his concurrence in *Riley*, Justice Alito suggested that the warrant requirement for cell phones would protect digital data in instances where hard-copy information would not be protected.[207] Accordingly, digital data found on a Connected Car might be

200 *Id.*

201 Mervosh, *supra* note 197.

202 Missouri v. McNeely, 569 U.S. 141, 154 (2013); *see id.* at 154 n.4.

203 *Id.* at 173 (Roberts, C.J., dissenting); *see* KAN. STAT. ANN. § 22-2504 (2016).

204 FED. R. CRIM. P. 4.1(a).

205 See Riley v. California, 134 S. Ct. 2473, 2493 (2014) (noting "Our cases have historically recognized that the warrant requirement is an important working part of our machinery of government, not merely an inconvenience to be somehow weighed against the claims of police efficiency.") (internal quotation marks omitted).

206 *See id.* at 2495 (arguing "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the founders fought.").

207 *See id.* at 2497 (Alito, J., concurring).

protected in instances where it would not be protected in a traditional automobile.

Nonetheless, Justice Alito noted that there was no other "workable alternative," and this is also the case for Connected Cars.[208] Firstly, police officers need clear rules to determine how to do their jobs. Alito opined that it would take "many years for the courts to develop more nuanced rules" about searching a cell phone;[209] I anticipate the same with Connected Cars. In the interim, officers need to know how to approach a Connected Car search so that the evidence obtained is not suppressed later on. In fact, with reference to my Introduction scenario, a New York Assistant District Attorney opined that the marijuana recovered by the officer would very likely be suppressed.[210] Lastly, this counterargument ignores the greater privacy interests afforded to digital data on Connected Cars. As discussed earlier, constant technology changes allow the collection and storage of digital data on Connected Cars.[211] Also, this Connected Car warrant requirement categorically protects all data on the Car rather than favoring some types of data over others, which is in line with *Riley*'s categorical protection of digital data on cell phones.[212] As a result, this warrant requirement helps to maintain the balance between individual rights and police power.

IV. CONCLUSION

To protect the privacy interests of Connected Car owners, the Supreme Court should adopt a warrant requirement for the digital data on a Connected Car. This proposed warrant requirement gives the Court a framework to apply the Fourth Amendment to current and future IoT technologies. The warrant requirement also serves to maintain the balance of police power with the privacy interests of individuals. *Riley* already requires a warrant for cell-phone searches, so this warrant requirement merely

208 *Id.*

209 *Id.*

210 Telephone Interview with Assistant District Attorney, *supra* note 28.

211 *See supra* Part I.

212 Birchfield v. North Dakota, 136 S. Ct. 2160, 2176-77 (2016) (Thomas, J., concurring in part and dissenting in part) (noting that the *Riley* Court adopted a categorical approach by requiring a warrant for a search of any and all cell phone data).

provides the corollary for Connected Cars and other emerging IoT technologies.

This proposed warrant requirement should not be limited to Connected Cars; it is merely a starting point in the Fourth Amendment/IoT conversation. IoT technology will unquestionably continue to develop and pervade our everyday lives; Google Glasses, Virtual Reality headsets, and microchip implants will soon become commonplace. This pervasiveness permits intimate details of one's life to be aggregated in ways that have never been possible.

The Fourth Amendment has withstood the test of time, and it will also be a guide through this next chapter of progress. Requiring a warrant is the path that best protects the rights of individuals from over-encroachment by the government.