

3-15-2021

## New Technology and the Right to Privacy: Do E-Scooters Implicate the Fourth Amendment?

Alexander P. Carroll

Follow this and additional works at: <https://digitalcommons.pepperdine.edu/naalj>



Part of the [Administrative Law Commons](#), [Constitutional Law Commons](#), [Science and Technology Law Commons](#), and the [Transportation Law Commons](#)

### Recommended Citation

Alexander P. Carroll, *New Technology and the Right to Privacy: Do E-Scooters Implicate the Fourth Amendment?*, 40 J. Nat'l Ass'n Admin. L. Judiciary 27 (2021)

Available at: <https://digitalcommons.pepperdine.edu/naalj/vol40/iss2/2>

This Comment is brought to you for free and open access by the Caruso School of Law at Pepperdine Digital Commons. It has been accepted for inclusion in Journal of the National Association of Administrative Law Judiciary by an authorized editor of Pepperdine Digital Commons. For more information, please contact [Katrina.Gallardo@pepperdine.edu](mailto:Katrina.Gallardo@pepperdine.edu), [anna.speth@pepperdine.edu](mailto:anna.speth@pepperdine.edu), [linhgavin.do@pepperdine.edu](mailto:linhgavin.do@pepperdine.edu).

# **New Technology and the Right to Privacy: Do E-Scooters Implicate the Fourth Amendment?**

**Alexander P. Carroll**

I.	INTRODUCTION .....	28
II.	THE FOURTH AMENDMENT.....	28
III.	IN THE REAL WORLD .....	30
IV.	THE FOURTH AMENDMENT AND E-SCOOTERS? .....	32
V.	MOBILITY COMPANY RESPONSES.....	36
VI.	PRIVACY CONCERNS.....	37
VII.	RELATED LEGISLATION ISSUES.....	42
VIII.	RELATED LITIGATION .....	45
IX.	WHAT ARE THE BENEFITS OF THE MOBILITY DATA SPECIFICATION.....	46
X.	HOW DOES THE REQUIREMENT TO PROVIDE DATA RELATE TO THE FOURTH AMENDMENT? .....	47
XI.	SUGGESTIONS TO AVOID THE ISSUE .....	50
XII.	CONCLUSION.....	51

## I. INTRODUCTION

People have increasingly begun using e-scooters to commute in metropolitan areas. However, there may be an issue. Do people face privacy issues every time they ride e-scooters? While the Fourth Amendment protects people's right to privacy, this right has become increasingly complicated as society and technology have progressed. Courts have had to grapple with new technology to determine if it violates people's Fourth Amendment rights when the government uses that technology to gather personal information. Now courts must decide if tracking e-scooter rider locations violates the Fourth Amendment.

This article begins with an overview of the Fourth Amendment and situations that implicate it.<sup>1</sup> Then the article will provide a history of different issues that courts have struggled with regarding the Fourth Amendment.<sup>2</sup> This discussion will include cell phones and tracking devices government agencies have used to gather information against citizens.<sup>3</sup> It will also discuss situations that *do not* implicate Fourth Amendment privacy rights, even though the situations seem as if they should.<sup>4</sup>

This article will then continue to explain the main focus of the article: legislation implemented by some cities that requires e-scooter companies, and other dockless transportation services like e-bicycles, to collect trip data and return this data to the cities in exchange for operating permits.<sup>5</sup> This article will weigh the benefits of the law with the potential harms to users and discuss what, if anything, seems like a better solution.<sup>6</sup>

This article will compare the privacy implications of the new reporting laws to both prior legal government surveillance and illegal unconstitutional government surveillance.<sup>7</sup> This article will argue that the new reporting mandate does indeed implicate the Fourth Amendment.

## II. THE FOURTH AMENDMENT

To understand the privacy issues the new law implicates, it is first necessary to understand the origin of privacy concerns, which requires an understanding of the Fourth Amendment. In relevant part, the Fourth Amendment states that “[t]he right of the people to be secure in their persons houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause.”<sup>8</sup> But what does this mean for modern privacy implications? Who does the Fourth Amendment protect, and how are those people actually protected by the Fourth Amendment?

Determining who is protected under the Fourth Amendment is not as simple as one would expect. The Fourth Amendment does not apply to protect simply anyone who is physically within the United States; instead it protects those

---

<sup>1</sup> See *infra* sections I and II.

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

<sup>4</sup> See *infra* section II.

<sup>5</sup> See *infra* section III.

<sup>6</sup> See *infra* sections VIII, IX, and X.

<sup>7</sup> See *infra* section IX.

<sup>8</sup> U.S. CONST. amend. IV.

individuals who have “sufficient connection” to the country.<sup>9</sup> This does not necessarily mean that the person must be a citizen of the United States though—a non-citizen may have protection as well.<sup>10</sup> In order to determine if the Fourth Amendment protects a person, courts analyze whether the person “accepted some societal obligations.”<sup>11</sup>

The next issue is the scope of the Fourth Amendment’s protection. The Fourth Amendment only protects people from “governmental action.”<sup>12</sup> It does not protect against actions taken by a private person since the Fourth Amendment “was not intended to be a limitation upon other than governmental agencies.”<sup>13</sup> This means the Fourth Amendment protects from invasions of privacy carried out by government agencies such as police, other law enforcement agencies, or any other governmental agency.<sup>14</sup>

However, it is important to note the Fourth Amendment protects more than just actions by government agencies. The Fourth Amendment can control actions by private parties in certain situations.<sup>15</sup> For this to happen, the private actor must convert into a government actor.<sup>16</sup> This means that action by a private company can violate a person’s constitutional right to privacy.<sup>17</sup> This happens when the government requires or mandates the private company to perform the action on behalf of or at the behest of the government.<sup>18</sup> In order for the Fourth Amendment to apply, the government agency in question has to do “more than adopt a passive position toward the underlying private conduct.”<sup>19</sup>

This private action to government action conversion often occurs when governments show a “strong preference” that the surveillance take place.<sup>20</sup> A situation involving government “encouragement, endorsement, and participation” is sufficient to “implicate the Fourth Amendment.”<sup>21</sup> Additionally, a government mandate can show this sort of action.<sup>22</sup>

In summary, the Fourth Amendment protects individuals with sufficient connection to the country who suffer an invasion of privacy from a government actor, or a private actor acting on behalf of the government through a government mandate to perform surveillance.<sup>23</sup> Only if these requirements are fulfilled will a

---

<sup>9</sup> *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1989).

<sup>10</sup> *Id.* at 273.

<sup>11</sup> *Id.*

<sup>12</sup> *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921).

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*

<sup>15</sup> *Skinner v. Ry. Labor Exec.s’ Ass’n*, 489 U.S. 602, 614–16 (1989).

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> *Id.* at 615.

<sup>20</sup> *Id.*

<sup>21</sup> *Id.* at 616.

<sup>22</sup> *Id.*

<sup>23</sup> *See, e.g., United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1989); *Skinner v. Ry. Labor Exec.s’ Ass’n*, 489 U.S. 602, 614–16 (1989); *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921).

person have any claim against the company or government for intrusion on their Fourth Amendment right to privacy.<sup>24</sup>

### III. IN THE REAL WORLD

Although the application of the aforementioned principles does not seem difficult, it can be more complicated than it seems. One situation worth discussing is the use of cell site location information to gather information in *Carpenter v. United States*.<sup>25</sup> There, police tried to determine the identity of the perpetrator who committed several robberies over the course of four months.<sup>26</sup> In order to find out this information, the police used cell site location data to determine who was near the crime scene at the time the crime occurred.<sup>27</sup> The police discovered one of their suspects was contacted by a new phone number, and that new phone number's user was near the crime scene at the time the crime occurred.<sup>28</sup>

The Court determine that cell phone monitoring violated the individual's right to privacy.<sup>29</sup> The Court stated that generally, people do not have a reasonable expectation of privacy in their movement in public places, so the use of cell cite location data to determine an individual's location in public is not necessarily an issue on its face.<sup>30</sup> However the Court held that because the monitoring was so precise and that it occurred over a long period of time there was a privacy issue.<sup>31</sup> Even though it tracked movements visible in public, the level of detail and duration converted a potentially constitutional observation into an unconstitutional observation.<sup>32</sup>

Two other cases that are related to this issue are best viewed side-by-side. The first case ruled there was no constitutional issue with the monitoring,<sup>33</sup> and the second ruled there was a constitutional issue.<sup>34</sup> First, we will discuss *United States v. Knotts*, where the court ruled no Fourth Amendment issue occurred.<sup>35</sup> In that case, the police suspected an individual of manufacturing illegal drugs.<sup>36</sup> In order to determine if this suspicion was correct, they tracked a container of chemicals implanted with a radio transmitter from the chemical production company to a cabin where the defendants were staying.<sup>37</sup>

For the same reasons that the Court ruled that *Carpenter* was a constitutional violation, the Court ruled that this form of monitoring did *not* violate the Constitution.<sup>38</sup> The use of the technology only allowed law

---

<sup>24</sup> *Id.*

<sup>25</sup> *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

<sup>26</sup> *Id.* at 2211–12.

<sup>27</sup> *Id.* at 2213.

<sup>28</sup> *Id.*

<sup>29</sup> *Id.* at 2217.

<sup>30</sup> *Id.* at 2215.

<sup>31</sup> *Id.* at 2216.

<sup>32</sup> *Id.* at 2216–17.

<sup>33</sup> *United States v. Knotts*, 460 U.S. 276, 285 (1983).

<sup>34</sup> *United States v. Karo*, 468 U.S. 705, 713–18 (1984).

<sup>35</sup> *Knotts*, 460 U.S. at 285.

<sup>36</sup> *Id.* at 280–85.

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

enforcement to track the vehicle carrying the contraband on public roads.<sup>39</sup> This monitoring could have been conducted without the radio transmitter, so the fact that they used that technology did not change anything.<sup>40</sup> The court stated while this is a very efficient means of conducting the observation, it was not so intrusive as to be a constitutional violation.<sup>41</sup> It is important that this tracking did not reveal any information that could not have been seen with the naked eye.<sup>42</sup>

*United States v. Karo* exemplifies the other side of this issue.<sup>43</sup> This case involved using the same radio transmitter technology as *Knotts*.<sup>44</sup> In this case, as well, law enforcement tracked a package along public roads.<sup>45</sup> The court did not consider this aspect of the case to be an issue; however, the government also tracked the package once it went into the suspects' house.<sup>46</sup> This fact differentiates the two cases.

The court found that this created a Fourth Amendment issue because it showed information about the interior of the home where there is a protected privacy interest.<sup>47</sup> These two cases demonstrate that monitoring people in public for a short time is acceptable, but once the monitoring starts to invade private areas, it is no longer acceptable under the Fourth Amendment.

Perhaps the most crucial case related to the central issue of this article is *United States v. Jones*.<sup>48</sup> That case involved an individual who the police suspected of trafficking narcotics.<sup>49</sup> To investigate their suspicions, the police attached a GPS device to the bottom of the suspect's wife's car, tracked the car's movements on public highways for thirty days, and then compiled all of that location information.<sup>50</sup> The defendant argued that the police violated his Fourth Amendment right.<sup>51</sup> The government counter-argued that it was not a search because they only tracked the vehicle while it was on "public roads, which were visible to all."<sup>52</sup> The government argued that because the car was on public roads and anyone could see it, it was not a constitutional violation.<sup>53</sup>

The majority opinion only addressed whether the police violated the Fourth Amendment by physically intruding on the vehicle to install the GPS device.<sup>54</sup> The concurring opinions went further, however, arguing that a reasonable person would not expect to be continuously followed for such a long

---

<sup>39</sup> *Id.*

<sup>40</sup> *Id.*

<sup>41</sup> *Id.*

<sup>42</sup> *Id.*

<sup>43</sup> *Karo*, 468 U.S. at 713–18.

<sup>44</sup> *Id.* at 708.

<sup>45</sup> *Id.* at 713–18.

<sup>46</sup> *Id.*

<sup>47</sup> *Id.*

<sup>48</sup> *United States v. Jones*, 565 U.S. 400 (2012).

<sup>49</sup> *Id.* at 402–03.

<sup>50</sup> *Id.*

<sup>51</sup> *Id.*

<sup>52</sup> *Id.* at 406.

<sup>53</sup> *Id.*

<sup>54</sup> *Id.* at 404–11.

period of time.<sup>55</sup> The concurrence posited that this type of continued surveillance did more than merely show the path a person took each day.<sup>56</sup> By compiling extensive travel data about a person, the government is able to collect intimate information about people.<sup>57</sup> When the government records a person's location for a long period of time, they are able to determine information about the person such as their professional associations, religious leanings, sexual associations, and familial associations.<sup>58</sup> The theory is that each piece of information comes together to paint a picture that reveals intimate details of the person's life and is thus a violation of their privacy.<sup>59</sup>

A helpful way to understand how many small pieces of information may add up to enough information to be a constitutional violation comes from a philosophical thought experiment known as the Sorites Paradox.<sup>60</sup> This thought experiment calls for a person to attempt establish at what point *individual* pieces of grain become a *heap* of grain.<sup>61</sup> The issue is that there is no obvious point when a group of individual pieces of grain becomes a heap.<sup>62</sup> This concept applies to the issue which the concurring Justices struggled with in *Jones*. A court must determine how many pieces of information about a person reaches the point where the government has enough to violate the person's reasonable expectation of privacy. Each piece of information about where a person has been by itself is not important, but when the pieces are taken together, they may reveal intimate details of that person's life, which constitutes a legitimate invasion of privacy.

#### IV. THE FOURTH AMENDMENT AND E-SCOOTERS?

What do these cases and the Fourth Amendment have to do with e-scooters? When these e-scooters were just a simple way to get around in cities, then they had nothing to do with the Fourth Amendment. However, some cities across the country have new regulations regarding e-scooters that may raise constitutional concerns.<sup>63</sup>

As populations continue to grow, cities will only become busier. In cities like Los Angeles, normal automobile traffic continues to worsen and ride share services like Lyft and Uber also crowd the road.<sup>64</sup> Further, public transportation

---

<sup>55</sup> *Id.* at 418–31.

<sup>56</sup> *Id.*

<sup>57</sup> *Id.*

<sup>58</sup> *Id.*

<sup>59</sup> *Id.*

<sup>60</sup> *Sorites Paradox*, STAN. ENCYCLOPEDIA OF PHIL. (Mar. 26, 2018), <https://plato.stanford.edu/entries/sorites-paradox/>.

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

<sup>63</sup> *Members*, OPEN MOBILITY FOUND., <https://www.openmobilityfoundation.org/members/> (last visited Mar. 22, 2020) (noting that the cities that have joined Open Mobility as of 2/20/2020 are Austin, Texas; Louisville, Kentucky; Miami-Dade, Florida; Philadelphia, Pennsylvania; San Jose, California; Washington, District of Columbia; Los Angeles, California; Minneapolis, Minnesota; Portland, Oregon; Santa Monica, California; Chicago, Illinois; Miami, Florida; New York City, New York; San Francisco, California; and Seattle, Washington.)

<sup>64</sup> Aarian Marshall, *Why Uber is Fighting Cities Over Data on Scooter Trips*, WIRED (May 13, 2019, 7:00 AM), <https://www.wired.com/story/why-uber-fighting-cities-data-about-scooters/>.

and pedestrians contribute to the chaos.<sup>65</sup> Cities will become even more congested as new technology is developed and becomes more common.<sup>66</sup> Thus, cities want to ensure they are operating as efficiently as possible, and that all available transportation products are accessible to as many people as possible.<sup>67</sup> In order to achieve these goals, cities must collect data.<sup>68</sup> They need the data not only to determine how to allocate funds for infrastructure, but also to ensure that companies are placing the mobility products evenly throughout different income areas.<sup>69</sup>

Early in 2019, an article introduced a new mandate implemented in Los Angeles, California.<sup>70</sup> The article starts out light heartedly and states: “Los Angeles is very nosy about where people are going to be dorkily bopping around on e-scooters.”<sup>71</sup> Subsequently, the article explains the real issue behind the mandate. The city will only allow e-scooter companies to place their products within the city if they agree to provide e-scooter location data to the city.<sup>72</sup> To “operate in Los Angeles[,] . . . the firms had to agree to allow the city to share anonymized data, updated every 24 hours, on where each scooter or bike trip starts, where it ends, and its route through the city.”<sup>73</sup>

Seleta Reynolds, the General Manager of the Los Angeles Department of Transportation (LADOT), spoke at MWC Barcelona, a conference for new technologically-advanced city planning ideas.<sup>74</sup> She spoke about how LADOT’s new program is developed to manage and keep track of e-scooters and other micromobility devices.<sup>75</sup> The program is called “Mobility Data Specification,” and it is “comprised of a set of Application Programming Interfaces (APIs) that create standard communications between cities and private companies to improve their operations.”<sup>76</sup> The program “allow[s] cities to collect data that can inform real-time traffic management and public policy decisions to enhance safety, equity and quality of life.”<sup>77</sup> The city states that the purpose of the new mandate is to allow the city to operate smoothly and successfully manage the congestion that comes with a large population.<sup>78</sup> Among other things, the city would use the

---

<sup>65</sup> *Id.*

<sup>66</sup> *Id.*

<sup>67</sup> *Id.*

<sup>68</sup> *Id.*

<sup>69</sup> *Id.*

<sup>70</sup> Jason Torchinsky, *Los Angeles Says E-Scooter Companies Have to Share Location Data*, JALOPNIK (Mar. 22, 2019, 11:11 AM), <https://jalopnik.com/los-angeles-says-e-scooter-companies-have-to-share-loc-1833490770>.

<sup>71</sup> *Id.*

<sup>72</sup> *Id.*

<sup>73</sup> Marshall, *supra* note 64.

<sup>74</sup> Amy Nordrum, *Los Angeles to Require Scooter Companies to Share Data*, IEEE SPECTRUM (Feb. 19, 2019, 20:30 GMT), <https://spectrum.ieee.org/telecom/wireless/mwc-barcelona-2019-los-angeles-to-require-scooter-companies-to-share-data>.

<sup>75</sup> *Id.*

<sup>76</sup> *Global Coalition of Cities Launches the ‘Open Mobility Foundation’*, OPEN MOBILITY FOUND. (Jun. 25, 2019), [https://www.openmobilityfoundation.org/wp-content/uploads/2019/10/OpenMobilityFoundationLaunch\\_NewsRelease\\_25June2019\\_final2-1.pdf](https://www.openmobilityfoundation.org/wp-content/uploads/2019/10/OpenMobilityFoundationLaunch_NewsRelease_25June2019_final2-1.pdf).

<sup>77</sup> *Id.*

<sup>78</sup> Nordrum, *supra* note 74.

information to determine where scooters are and what areas need more devices.<sup>79</sup> The purpose of having the data is to integrate “all of [the] information into a dashboard that would display all public and private transportation options that are currently in use throughout the city.”<sup>80</sup> Ultimately, the goal is to make traveling safer and easier for everyone in the city.<sup>81</sup>

What sort of information do cities want to collect? LADOT and other cities implementing the regulations require companies to turn over “[r]oute information ... after the trip has completed and within 24 hours [that] doesn’t include the name, age, gender, address of the user.”<sup>82</sup> The cities also require “companies to provide the start trip and end trip of every vehicle as trips start and trips end to make sure scooters are being parked legally and within the terms of the permit.”<sup>83</sup> The cities requires the data to be turned over, or else they will not provide operating permits for the companies to place their scooters in the city.<sup>84</sup> The cities claim they can do this because they have “direct regulatory authority over their sidewalks, where the shared scoots need to park.”<sup>85</sup>

The City of Santa Monica, California issued a report detailing information regarding the new policy surrounding the e-scooters and e-bikes.<sup>86</sup> The report discussed the city's planned treatment of mobility device data.<sup>87</sup> The report also discussed tracking e-scooters and e-bikes.<sup>88</sup> The city states that “[i]t is preferred that devices have enhanced GPS equipment that provides the locational accuracy needed to virtually designate a ‘hub’ or ‘station’ system for device parking, to track trip path, to restrict speed in designated areas.”<sup>89</sup> Santa Monica also states they are not collecting any user's personal information.<sup>90</sup>

California cities are not the only cities requiring mobility device data to be turned over in exchange for a license to operate dockless vehicles.<sup>91</sup> Austin, Texas is adopting similar requirements. To operate e-scooters within the city, companies must report trip data to the city.<sup>92</sup> In a report Austin released, the city states a “[l]icensee shall provide the Director ... with real-time and historical information

---

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

<sup>81</sup> *Id.*

<sup>82</sup> Alfred Ng, *The Majority of Scooters in LA Are Going to Share Your Location with the City*, CNET (Mar. 22, 2019, 11:39 AM), <https://www.cnet.com/news/the-majority-of-scooters-in-la-are-going-to-share-your-location-with-the-city/>.

<sup>83</sup> *Id.*

<sup>84</sup> *Id.*

<sup>85</sup> Aarian Marshall, *Still Smarting from Uber, Cities Wise up About Scooter Data*, WIRED (Sept. 18, 2018, 7:00 AM), <https://www.wired.com/story/cities-scooter-data-remix-uber-lyft/>.

<sup>86</sup> *City of Santa Monica Shared Mobility Device Pilot Program Administrative Regulations*, CITY OF SANTA MONICA (Aug. 1, 2018), <https://www.smgov.net/uploadedFiles/Departments/PCD/Transportation/Regulartors.pdf>.

<sup>87</sup> *Id.*

<sup>88</sup> *Id.*

<sup>89</sup> *Id.*

<sup>90</sup> *Id.*

<sup>91</sup> *Shared Mobility Services*, AUSTINTEXAS.GOV, <http://austintexas.gov/micromobility> (last visited Feb. 22, 2020).

<sup>92</sup> *Memorandum Dockless Mobility Rules Update*, CITY OF AUSTIN (Nov. 9, 2018), [www.austintexas.gov/edims/pio/document.cfm?id=310384](http://www.austintexas.gov/edims/pio/document.cfm?id=310384).

for their entire fleet through a documented web-based application programming interface.”<sup>93</sup> The city also emphasizes that they have privacy safeguards in place to protect the identities of users.<sup>94</sup>

After the LADOT developed their initial program, “Mobility Data Specification,” the program started to gain traction and more cities than Santa Monica and Austin began using it.<sup>95</sup> In fact, more than fifty cities across the United States began using the MDS program.<sup>96</sup> In June 2019, the “Open Mobility Foundation” (OMF) was formed.<sup>97</sup> The OMF began managing the original LADOT Mobility Data Specifications program and partnered with OASIS, a company that hosted and allowed municipalities to use the program to manage their cities.<sup>98</sup> Currently, the United States members of the OMF include: San Diego, California; Long Beach, California; San Jose, California; Los Angeles, California; San Francisco, California; Santa Monica, California; Detroit, Michigan; Denver, Colorado; Columbus, Ohio; Pittsburg, Pennsylvania; Philadelphia, Pennsylvania; Austin, Texas; Louisville, Kentucky; Miami-Dade, Florida; Miami, Florida; Washington DC; Minneapolis, Minnesota; Portland, Oregon; Chicago, Illinois; New York City, New York; and Seattle, Washington.<sup>99</sup>

All of these cities enact these regulations and require access to the dockless vehicles' routes and end locations so they can attempt to organize their city and help it run as smooth as possible. They want to use the program to “determine who’s adhering to the regulations and whether they’re complying.”<sup>100</sup> Does a city need to know a micromobility device's trip data to run the city efficiently? Is there some other way to make sure there are scooters in the right area without recording of the citizens trip data when they ride e-scooters?

---

<sup>93</sup> *Director Rules for Deployment and Operation of Shared Small Vehicle Mobility Systems*, AUSTIN TRANSP. DEP’T. 10, [https://austintexas.gov/sites/default/files/files/Transportation/Dockless\\_Final\\_Accepted\\_Searchable.pdf](https://austintexas.gov/sites/default/files/files/Transportation/Dockless_Final_Accepted_Searchable.pdf) (last visited Feb. 22, 2020).

<sup>94</sup> *Id.* at 9.

<sup>95</sup> *Global Coalition of Cities Launches the ‘Open Mobility Foundation’*, *supra* note 76.

<sup>96</sup> *Id.*

<sup>97</sup> *Id.*

<sup>98</sup> *Id.*

<sup>99</sup> *Members*, *supra* note 63.

<sup>100</sup> Marshall, *supra* note 85.

## V. MOBILITY COMPANY RESPONSES

There are several primary mobility companies that provide e-scooter and e-bike services.<sup>101</sup> While the regulation has the same impact on how the companies can operate their business, there are varying reactions to the new legislation.<sup>102</sup>

Uber, a large player in the alternate transportation industry, is not supportive of the new rules because they do not want to turn over the location data.<sup>103</sup> Uber fought back against the regulations and the Department of Transportation thereby granted them only a temporary operating permit in Los Angeles because they would not agree to turning over the location data.<sup>104</sup> Uber's issue with the new regulations is the privacy implications it has for their customers.<sup>105</sup> Uber told Motherboard, the technology division of Vice News, that "[u]nder current and proposed privacy legislation in the United States, private companies are expected to demonstrate specific data security and privacy capabilities when dealing with personal information, including GPS data."<sup>106</sup> This legislation seems beneficial and that it would limit potential privacy issues, however Uber's statement indicates that the e-scooter issue may be larger than it seems. Uber told Motherboard: "Despite repeated attempts by Uber and consumer advocacy groups, we've received no assurance that LADOT is willing or able to meet the same standard in protecting the privacy of our customers."<sup>107</sup>

Uber is concerned that this data collection "constitutes government surveillance, and would yield far more information about bicyclists and scooter riders than is available for drivers or transit commuters."<sup>108</sup> In a letter to Reynolds, Uber said that it was a "*massive overcollection* of data about the movements of bike and scooter users."<sup>109</sup> However, Uber's worries extend past scooters.<sup>110</sup> The company fears that "cities like LA may begin to demand user data on other modes of transportation."<sup>111</sup> The company released a statement saying they "are concerned that privacy-violating provisions of MDS will be expanded to other modes of transportation."<sup>112</sup>

Lime, one of the other major micromobility companies, is more supportive of the regulations requiring sharing location data.<sup>113</sup> Lime explained to

---

<sup>101</sup> Joseph Cox, *Scooter Companies Split on Giving Real-Time Location Data to Los Angeles*, VICE (Mar. 19, 2019, 5:43 AM), [https://www.vice.com/en\\_us/article/yw8j5x/scooter-companies-location-data-los-angeles-uber-lyft-bird-lime-permits](https://www.vice.com/en_us/article/yw8j5x/scooter-companies-location-data-los-angeles-uber-lyft-bird-lime-permits).

<sup>102</sup> *Id.*

<sup>103</sup> *Id.*

<sup>104</sup> *Id.*

<sup>105</sup> *Id.*

<sup>106</sup> *Id.*

<sup>107</sup> Cox, *supra* note 101.

<sup>108</sup> Laura J. Nelson, *Data Privacy Debate Emerges Out of L.A.'s Scooter Craze*, GOVERNMENT TECHNOLOGY (Mar. 18, 2019) <https://www.govtech.com/transportation/Data-Privacy-Debate-Emerges-Out-of-LAs-Scooter-Craze.html>.

<sup>109</sup> Marshall, *supra* note 64.

<sup>110</sup> *Id.*

<sup>111</sup> *Id.*

<sup>112</sup> *Id.*

<sup>113</sup> Cox, *supra* note 101.

Motherboard that “Los Angeles serves as a valuable model for other communities and is a real solution to easing congestion, curbing pollution and increasing mobility options.”<sup>114</sup> Lime supported making the products safer and ensuring the products reach more people who may need them.<sup>115</sup> However, they failed to address Uber's privacy concerns.<sup>116</sup>

Bird, another micromobility company, also gave a statement to Motherboard addressing the new Department of Transportation regulations as well as addressing potential privacy concerns.<sup>117</sup> Bird said, “[f]rom the beginning, Bird has been steadfastly committed to the privacy of our riders. We want to partner with cities as they build and improve their infrastructure so that e-scooters and other micromobility options are available and safer for more people, while ensuring the privacy of our riders.”<sup>118</sup> Bird further expressed that it “look[s] forward to continuing to work with LADOT and other cities on the responsible implementation of mobility management tools and data sharing.”<sup>119</sup> Bird’s trust of LADOT and the OMF with its customer’s privacy is implicit in this statement, in contrast to Uber. Further showing the trust in the regulations, Bird is a member of the OMF.<sup>120</sup>

Lyft did not give a statement about the new legislation<sup>121</sup> but like Uber, supports “legislation that would restrict what kinds of data cities are allowed to collect.”<sup>122</sup>

The companies controlled by these new regulations are not the only ones who have made statements regarding the potential privacy issues. These concerns are explored in the next section.

## VI. PRIVACY CONCERNS

Jason Torchinsky concludes his article, *Los Angeles Says E-Scooter Companies Have to Share Location Data*, by stating, “more data in more hands means more potential for risk.”<sup>123</sup> This statement clearly states the concerns that many people have. The author posits that the regulations and the benefits are reasonable but “concerns about user privacy are real.”<sup>124</sup> This author is just one of many who has concerns. The City of Los Angeles attempted to alleviate some of these concerns and promised “to aggregate the anonymized data, de-identifying and destroying the information it did not need. It would only allow law enforcement access to the info through subpoena. And the city pledged to be very

---

<sup>114</sup> *Id.*

<sup>115</sup> *Id.*

<sup>116</sup> *Id.*

<sup>117</sup> *Id.*

<sup>118</sup> *Id.*

<sup>119</sup> *Id.*

<sup>120</sup> *Members, supra* note 63.

<sup>121</sup> *Id.*

<sup>122</sup> Aarian Marshall, *These Cities Will Track Scooters to Get a Handle on Regulation*, WIRED (June 25, 2019, 6:36 PM) <https://www.wired.com/story/these-cities-will-track-scooters-handle-regulation/>.

<sup>123</sup> Torchinsky, *supra* note 70.

<sup>124</sup> *Id.*

careful before releasing any trip info to the public.”<sup>125</sup> However, many are still worried about the potential privacy violations.

One organization that objects to the data collection is the “Electronic Frontier Foundation” (EFF), a nonprofit that defends “digital privacy, free speech, and innovation.”<sup>126</sup> The EFF became involved because data collection raises privacy concerns. The EFF addresses the privacy concerns surrounding micromobility devices head-on and talks about privacy problems related to their data collection.<sup>127</sup>

The EFF accepts that the cities could remove personally identifiable information, but it says that the removal does not remedy the privacy concerns.<sup>128</sup> The EFF says that when consumers use e-scooters or other micromobility devices habitually, it is extremely easy to reidentify the individual users.<sup>129</sup> The organization discusses privacy issues similar to those recognized in the *Jones* concurrence.<sup>130</sup> The discussion says that “[t]ime-stamped geolocation data could also reveal trips to medical specialists, specific places of worship, and particular neighborhoods or bars.”<sup>131</sup> In other words, the tracking could gather intimate information that invades a user’s privacy. The collection is also an issue because as long as the cities have data, other organizations, such as law enforcement agencies or other third parties, could then reidentify the user.<sup>132</sup>

The Center for Democracy and Technology (CDT) also spoke out against the e-scooter data collection.<sup>133</sup> The CDT is a group that works to defend online civil liberties and human rights.<sup>134</sup> The organization tries to solve policy issues related to the internet.<sup>135</sup> One of the organization’s pillars is limiting government surveillance.<sup>136</sup> In a letter to the LADOT regarding the Mobility Data Specification program, the CDT warned that the data being collected was extremely sensitive and therefore the collection must be justified and limited in a correct manner as to not create privacy issues.<sup>137</sup>

---

<sup>125</sup> Marshall, *supra* note 64.

<sup>126</sup> ELECTRONIC FRONTIER FOUNDATION, <https://www.eff.org/> (last visited Feb. 23, 2020).

<sup>127</sup> Jamie Williams, *Five California Cities Are Trying to Kill an Important Location Privacy Bill*, ELECTRONIC FRONTIER FOUNDATION (Jun. 10, 2019), <https://www.eff.org/deeplinks/2019/06/five-california-cities-are-trying-kill-important-location-privacy-bill>.

<sup>128</sup> *Id.*

<sup>129</sup> *Id.* When a rider uses scooters as their main means of transportation, this increases the likelihood of reidentification because there are more data points to base the reidentification off of.

<sup>130</sup> *United States v. Jones*, 565 U.S. 400 (2012).

<sup>131</sup> Williams, *supra* note 127.

<sup>132</sup> *Id.*

<sup>133</sup> Natasha Duarte and Joseph Jerome, *Comments to LADOT on Privacy & Security Concerns for Data Sharing for Dockless Mobility*, CENTER FOR DEMOCRACY & TECHNOLOGY (Nov. 29, 2018), <https://cdt.org/insights/comments-to-ladot-on-privacy-security-concerns-for-data-sharing-for-dockless-mobility/>.

<sup>134</sup> *Who We Are*, CENTER FOR DEMOCRACY & TECHNOLOGY, <https://cdt.org/who-we-are/> (last visited Feb. 23, 2020).

<sup>135</sup> *Id.*

<sup>136</sup> *Id.*

<sup>137</sup> Duarte and Jerome, *supra* note 133.

The CDT explains that location data is very sensitive, “especially when collected over extended periods of time.”<sup>138</sup> The CDT also shares the concern that “[p]eople’s movements from place to place can reveal sexual partners, religious activities, and health information.”<sup>139</sup> The organization adds that the “U.S. Supreme court has recognized a strong privacy interest in location data, holding that historical cell cite location information is protected by the Fourth Amendment warrant requirement.”<sup>140</sup> The organization recognizes that LADOT has marked the information as confidential, but calls for them to provide more information including “how it will safeguard MDS data, including how long it will retain the data; the specific purposes for which the data will be used; and how the department will limit access and use to those specific purposes.”<sup>141</sup>

The CDT goes into detail about the privacy issues, and explains that even though the data is considered anonymous, there are still privacy implications recognized by other government authorities.<sup>142</sup> The CDT identifies issues with what the mandate considers not collecting any personal identifiable information (PII).<sup>143</sup> The data collecting program does not require the individual’s names to be turned over, but this is not the only PII.<sup>144</sup> “MDS trip data includes the precise start and end times and locations of trips, tied to persistent, unique device identifiers (UDIDs) for each bike or scooter. UDIDs can be PII.”<sup>145</sup> This is an issue because “according to the Federal Trade Commission (FTC), persistent identifiers like UDIDs, MAC addresses, and static IP addresses are often reasonably linkable to a particular person, computer, or device” and even the California Consumer Privacy Act often recognized UDIDs as PII.<sup>146</sup> When more information is connected to the UDID, such as location and trip information, “individuals can be personally identified with reasonable ease.”<sup>147</sup>

The CDT refers to an experiment by Anthony Tockar to support of their claim.<sup>148</sup> Tocker is a data scientist, who holds a Master’s of Science Degree in Analytics from Northwestern University.<sup>149</sup> Tockar’s experiment proved that he could identify individuals with di-identified trip data from New York’s Taxi and Limousine Commission.<sup>150</sup> In that experiment, Tockar only had a few data points

---

<sup>138</sup> *Id.*

<sup>139</sup> *Id.*

<sup>140</sup> *Id.*

<sup>141</sup> Duarte and Jerome, *supra* note 133.

<sup>142</sup> *Id.*

<sup>143</sup> *Id.*

<sup>144</sup> *Id.*

<sup>145</sup> *Id.*

<sup>146</sup> *Id.*

<sup>147</sup> *Id.*

<sup>148</sup> *Id.*

<sup>149</sup> Anthony Tockar, LINKEDIN, <https://www.linkedin.com/in/anthony-tockar-474a7252/?originalSubdomain=au> (last visited Feb. 23, 2020) (Tockar is the director and founder of Verge Labs. “Verge Labs is a new type of AI company focused on the applied side of machine learning. Our team of best-in-class data scientists sift through the daily firehose of theoretical research to build a curated library of techniques and utilities ready to be switched on at companies today.”).

<sup>150</sup> Duarte and Jerome, *supra* note 133.

but was still able to determine the individual taxi rider's identity.<sup>151</sup> The information that is collected for the scooter management system is more detailed than the information that Tockar used.<sup>152</sup> The location data that the MDS collects is more detailed because it records locations from the trip extremely close to where the rider starts and ends.<sup>153</sup> The MDS does not have to take into account limitations that come with tracking cars, such as parking constraints, which cause the trips to end further from the actual destination.<sup>154</sup> Since Tockar was successfully able to re-identify individuals with only limited data points, it could be much easier with the detailed data collected from the scooter trips.

The CDT brings up some concerns they believe could arise if the data banks possibly reached the wrong hands.<sup>155</sup> They are concerned that “[o]verbroad tracking could itself become a barrier to entry for low-income and minority riders, who already face disproportionate surveillance and scrutiny from law enforcement and other authorities. Without appropriate safeguards restricting access to the data, its collection could deter underserved riders.”<sup>156</sup> In addition, the CDT discuss past misuse of private data-bases. They report that “[r]ide-sharing APIs have been abused for things like spying on ex-partners, and a 2016 Associated Press study found that law enforcement officers across the country abused police databases to stalk romantic partners, journalists, and business associates.”<sup>157</sup> While these concerns are not confirmed, they are important issues that should be considered when deciding to make this a policy standard across the country, as this has become.<sup>158</sup>

The New York Times published an article that addressed an issue that is analogous to the one at hand.<sup>159</sup> The article explains how anonymous data is not truly anonymous, and is actually very personal data.<sup>160</sup> The article describes how applications installed on your phone track your location, sometimes even every few minutes.<sup>161</sup> According to some businesses that receive the data, it is easy to determine individual's identity based on that data.<sup>162</sup> The Times conducted an experiment on their own, in which they reviewed anonymous location data and

---

<sup>151</sup> *Id.*

<sup>152</sup> *Id.*

<sup>153</sup> *Id.*

<sup>154</sup> *Id.*

<sup>155</sup> *Id.*

<sup>156</sup> *Id.*

<sup>157</sup> *Id.*; see also Sadie Gurman, *AP: Across US, police officers abuse confidential databases*, THE ASSOCIATED PRESS (Sept. 27, 2016), <https://apnews.com/699236946e3140659fff8a2362e16f43/ap-across-us-police-officers-abuse-confidential-databases>.

<sup>158</sup> *Global Coalition of Cities Launches the 'Open Mobility Foundation'*, *supra* note 79. The Open Mobility Foundation took control of the program that LADOT started, and is now partnered with many cities across the country who all use the Mobility Data Specification program to track the scooters that are in their cities.

<sup>159</sup> Jennifer Valentino-Devries, Natasha Singer, Michael H. Keller and Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, THE NEW YORK TIMES (Dec. 10, 2018), <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>.

<sup>160</sup> *Id.*

<sup>161</sup> *Id.*

<sup>162</sup> *Id.*

determined the individual's identity, where she went for doctor's appointments, where she went to a Weight Watchers meeting, and when she stayed at her ex-boyfriends house.<sup>163</sup> The individual who was identified allowed The Times to conduct experiment and commented on the experiment.<sup>164</sup> She said "It's the thought of people finding out those intimate details that you don't want people to know."<sup>165</sup> While this is different than the scooter trip information, it provides another example of how anonymous data can be used to ascertain people's identity's and intimate details about them.<sup>166</sup> Similar to the previous cases, data that can determine intimate details about a person may be considered an unconstitutional government surveillance.<sup>167</sup>

In The Times article, they state that "[t]here is no federal law limiting the collection or use of such data."<sup>168</sup> While the data collection just described seems nearly identical to the Data Mobility System's requirements, there are key differences. This article will explain why the data collection just described is legal, whereas the Data Mobility System is not legal in a later section.<sup>169</sup>

The Times article is not the only source to show the supposedly anonymous data is not actually private. A scientific study published in 2013 shows that even coarse, non-specific data could reidentify an individual with significant ease.<sup>170</sup>

The researchers found that people's movements were generally highly unique and because of this, found that "this uniqueness means that little outside information is needed to re-identify the trace of a targeted individual even in a sparse, large-scale and coarse mobility dataset."<sup>171</sup>

This study "was performed using an anonymized mobile phone dataset that contains call information for ~1.5 M users of a mobile phone operator."<sup>172</sup> "Each time a user interacts with the mobile phone operator network by initiating or receiving a call or a text message, the location of the connecting antenna is recorded."<sup>173</sup> Even with this lower level of specificity, it was "enough to uniquely identify 95% of the individuals."<sup>174</sup> Comparing this to the very specific real-time location data that the micromobility companies are required to submit, it is evident that re-identification is an important concern.

---

<sup>163</sup> *Id.*

<sup>164</sup> *Id.*

<sup>165</sup> *Id.*

<sup>166</sup> *Id.*

<sup>167</sup> *United States v. Jones*, 565 U.S. 400 (2012).

<sup>168</sup> Valentino-Devries, Singer, Keller and Krolik, *supra* note 159.

<sup>169</sup> *See infra* section IX.

<sup>170</sup> Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen and Vincent D. Blondel, *Unique in the Crowd: The privacy bounds of human mobility*, SCIENTIFIC REPORTS (Mar. 25, 2013), <https://www.nature.com/articles/srep01376>.

<sup>171</sup> *Id.*

<sup>172</sup> *Id.*

<sup>173</sup> *Id.*

<sup>174</sup> *Id.*

## VII. RELATED LEGISLATION ISSUES

As is clear from their public responses to the requirements of the program, Uber and Lyft do not support the requirement to report data in order to place their products within the limits of the local municipalities.<sup>175</sup> The companies opposing the new standard have done more than just release public statements voicing their opinions on the matter.<sup>176</sup> “Uber and some of its allies have begun to maneuver in state houses.”<sup>177</sup> They also supported state legislature that was favorable to them.<sup>178</sup> As of May 2019, Uber, Lyft, and Bird all supported California Assembly Bill 1112 which “would prohibit local authorities from requiring companies that offer shared scooters or bikes to submit data on individual trips.”<sup>179</sup> This, of course, would benefit the dockless mobility companies, and would allow them to distribute their scooters wherever they want. It would also avoid the issue that this article is talking about – forcing the scooter companies to turn over information due to a regulatory scheme.

California Assembly Bill 1112 is more important than a normal state legislature bill because “California has long been ground zero for new technologies” and legislature surrounding the new technology may set a precedent that other states will follow.<sup>180</sup> As mentioned, the LADOT was first to use the Mobility Data Specification before the Open Mobility Foundation took over its operation.<sup>181</sup> Considering the program started in Los Angeles and spread across the country, it is easy to see why this proposed California Bill has national implications as well. Other states will likely adopt similar legislation, just as they adopted the Mobility Data Specification from the LADOT and the Open Mobility Foundation.

Opponents of AB 1112 say that it would destroy the tool that LADOT established, and would stop policy makers from being able to use the data collected to decide “where to install a bike lane or how to ensure e-scooter availability in low-income communities.”<sup>182</sup> Opponents say that the Bill is a preemption, and is being used as a “tool for Republican state legislatures to block policies enacted by Democratic cities.”<sup>183</sup> They state that the micromobility companies should talk to the city municipalities, rather than taking “their case straight to Sacramento.”<sup>184</sup> The reason for this is because “shared mobility is a local jurisdictional matter. [C]ities are responsible for managing sidewalks, streets, and public spaces...[and] are responsible for the enforcement of and compliance with local and state laws that govern the public right-of-way.”<sup>185</sup> The

---

<sup>175</sup> See *supra* section IV.

<sup>176</sup> Marshall, *supra* note 64.

<sup>177</sup> *Id.*

<sup>178</sup> *Id.*

<sup>179</sup> *Id.*

<sup>180</sup> David Zipper, *The California Legislature Is Getting Played by Micromobility Companies*, CITYLAB (May 17, 2019), <https://www.citylab.com/perspective/2019/05/california-state-laws-shared-mobility-city-rules-ab-1112/589705>.

<sup>181</sup> *Global Coalition of Cities Launches the ‘Open Mobility Foundation’*, *supra* note 76.

<sup>182</sup> Zipper, *supra* note 180.

<sup>183</sup> *Id.*

<sup>184</sup> *Id.*

<sup>185</sup> *Id.*

opponents say this Bill would not allow “urban officials to harness the rapid evolution of mobility technology to promote safety and equitable access” which is a valid concern.<sup>186</sup> However, their concerns may be moot.

A closer look at the Bill itself shows that the concerns that the opponents had were uncalled for.<sup>187</sup> The California Legislative Information website shows the Bill, strikethroughs, and revisions.<sup>188</sup> The Bill originally was written to “prohibit a local authority from imposing any unduly restrictive requirements on mobility device providers that have the effect of prohibiting the operation of all shared mobility providers in its jurisdiction.”<sup>189</sup> However it was later amended to say that the Bill would “allow a local authority to enact reasonable regulations on shared mobility devices and providers within its jurisdiction, including, but not limited to, requiring a shared mobility service provider to obtain a permit.”<sup>190</sup> Thus, the Bill was originally a preemption tool, as the opponents worried; however, after the revision it would allow the local governments to control their jurisdiction as they saw fit. Further reason to not worry is that the majority vote on this Bill was to not enact it.<sup>191</sup>

However, a section was added to the California Vehicle code that directly addresses micromobility regulation. Section 39057 says that:

- (a) A local authority may enact reasonable regulations on shared mobility devices and providers within its jurisdiction, including, but not limited to, the following:
  - (1) Requiring that, before distribution of a shared mobility device, a shared mobility service provider shall enter into an agreement with, or obtain a permit from, the local authority with jurisdiction over the area.<sup>192</sup>

This section allows for the cities to require mobility companies, such as Uber and Lyft, to comply with the necessary requirements to obtain a permit to operate within the jurisdiction. In other words, this is state legislation that allows the MDS to be taken seriously, allowing local governments to enact their own city ordinances requiring the data to be shared with the local governments in exchange for a permit to operate. This Bill is not the only legislation that may be in play, however.

The California Electronic Communications Privacy Act (CalECPA) is an act that “fleshes out an individual’s right to privacy under the state constitution.”<sup>193</sup> The act is “designed to block law enforcement agencies from

---

<sup>186</sup> *Id.*

<sup>187</sup> Cal. Legis. Assemb. B. 1112, 2019–20 Reg. Sess. (Cal. 2019).

<sup>188</sup> *Id.*

<sup>189</sup> *Id.*

<sup>190</sup> *Id.*

<sup>191</sup> *Id.*

<sup>192</sup> *Id.*

<sup>193</sup> Laura Bliss, *A Controversial Scooter Data Tracking Program Gains Traction*, CITYLAB (Aug. 23, 2019), <https://www.citylab.com/transportation/2019/08/scooter-ride-mobility-data-privacy-laws-ecpa-los-angeles/596446/>.

accessing user data, including emails, text messages, and personal information stashed online, without a warrant.”<sup>194</sup> California is not the only state to have an act that does this: “[o]ther states, including Maine, Vermont, and Utah, have similarly clarified and bolstered existing federal privacy protections within their own borders.”<sup>195</sup> Some of the companies the Mobility Data Specification impacted took it upon themselves to go to the California Legislature to obtain the government’s opinion on the legality of the permit requirement.<sup>196</sup> The State Legislative Counsel, which interprets state statutes to help inform lawmakers on the legality of different issues, released their findings regarding the Mobility Data Specification.<sup>197</sup> The Counsel’s first finding was: “CalECPA restricts a local government agency, as a political subdivision of the state, from requiring the provision of real-time location data as a condition of an operating permit.”<sup>198</sup> The second finding was: “A government entity is exempted from this restriction if a specific rider directly consents to share their data—but not through a mobility operator as an intermediary.”<sup>199</sup>

The head of the Mobility Data Specification program, Seleta Reynolds, responded to the Legislative Counsel’s findings.<sup>200</sup> Her response is that CalECPA was meant to control law enforcement agencies.<sup>201</sup> She says:

CalECPA was not written to limit the actions of regulatory agencies or to control the regulation of dockless mobility devices in the public right-of-way by a local department of transportation. In fact, there is no mention in either the statutory text or legislative history of any intent by the Legislature to limit or restrict a government regulator from using electronic data within the course and scope of regulating entities that are not electronic communications services.<sup>202</sup>

However, this has not stopped some companies from continuing to fight the municipalities adopting the MDS.

---

<sup>194</sup> *Id.*

<sup>195</sup> *Id.*

<sup>196</sup> *Id.*

<sup>197</sup> *Id.*

<sup>198</sup> *Id.*

<sup>199</sup> *Id.*

<sup>200</sup> *Id.*

<sup>201</sup> *Id.*

<sup>202</sup> *Id.*

### VIII. RELATED LITIGATION

At first, Uber agreed to turn over the requested information, however the company decided that it did not want to comply and threatened to “[file] a lawsuit and temporary restraining order” against LADOT in October 2019.<sup>203</sup> Uber refuses to follow the requirements all the way and contends that these requirements that the city put in place “constitute surveillance.”<sup>204</sup> When the city threatened to remove their permit if they did not comply, Uber responded by saying: “[W]e will file a lawsuit and seek a temporary restraining order in the Los Angeles Superior Court, so that a judge will hear these concerns and prevent the Los Angeles Department of Transportation from suspending our permit to operate.”<sup>205</sup> Uber seems willing to work with the city, as long as they can protect “the data privacy and security of [their] riders.”<sup>206</sup> At the end of October 2019, Uber had not filed the lawsuit, but remained in talks with the LADOT.<sup>207</sup>

Subsequently, in March 2020, Uber filed a complaint in federal court against LADOT alleging the Mobility Data Specification violated the Fourth Amendment and that the tracking could reveal personal information about people “such as where they live and work, where they go for social or romantic interactions, and even what time they leave their office each day.”<sup>208</sup> Uber argues that the Mobility Data Specification is not useful for assisting the city “in planning bike lanes, or figuring out deployment patterns in different neighborhoods, or dealing with complaints about devices that are parked in the wrong place, or monitoring compliance with permit requirements.”<sup>209</sup> Instead, Uber argues, it is “a tool for surveillance.”<sup>210</sup>

In addition to Uber, the American Civil Liberties Union (“ACLU”) and the EFF also brought suit in federal court against LADOT for the same reasons.<sup>211</sup> The ACLU released a statement regarding the situation and said: “Renting an electric scooter should not give the government the right to trace your every move — where you start, where you end, and all stops, twists, and turns in between.”<sup>212</sup>

It is clear that the companies are suing LADOT based on their riders’ privacy rights, but LADOT claims there is no constitutional violation, but instead,

---

<sup>203</sup> Laura Bliss, *Uber’s Beef with L.A. Is Bigger Than Data*, CITYLAB (Oct. 29, 2019), <https://www.citylab.com/transportation/2019/10/uber-lawsuit-data-privacy-scooter-tracking-los-angeles/600985/>.

<sup>204</sup> *Id.*

<sup>205</sup> *Id.*

<sup>206</sup> *Id.*

<sup>207</sup> Alfred Ng, *Uber in talks with Los Angeles as scooter location data lawsuit looms*, CNET (Oct. 30, 2019, 8:43 AM), <https://www.cnet.com/news/uber-in-talks-with-los-angeles-as-scooter-location-data-lawsuit-looms/>.

<sup>208</sup> Chris Teale, *Uber sues LADOT over data-sharing requirements*, SMART CITIES DIVE (Mar. 26, 2020), <https://www.smartcitiesdive.com/news/uber-jump-sues-los-angeles-mobility-data-sharing-requirement/574893/>.

<sup>209</sup> *Id.*

<sup>210</sup> *Id.*

<sup>211</sup> *Rent a Scooter in L. A. and the City Government Knows Your Every Move*, ACLU SOUTHERN CALIFORNIA (June 8, 2020), <https://www.aclusocal.org/en/press-releases/privacy-lawsuit-your-scooter-gps-data-being-tracked>.

<sup>212</sup> *Id.*

the Mobility Data Specification serves the purpose of enabling the cities to run smoother.<sup>213</sup> But what are those benefits?

### IX. WHAT ARE THE BENEFITS OF THE MOBILITY DATA SPECIFICATION

Proponents of any new legislation must weigh the pros and cons to see if it is worth enacting. The benefits to the community should be considered to see if they outweigh the harm to the community. This article has covered the possible privacy issues in depth above<sup>214</sup> and has briefly mentioned benefits and the purpose of the program, but it has not discussed the benefits that the MDS could bring in much detail. Before we discuss the Fourth Amendment issues, and possible solutions, if any are needed, we must fully understand both sides of the coin.

The proponents of the program in place mainly point to benefits the city government would have in organizing the city.<sup>215</sup> The main organizer of the program, the Open Mobility Foundation, says the program will “allow cities to collect data that can inform real-time traffic management and public policy decisions to enhance safety, equity and quality of life.”<sup>216</sup>

The chief sustainability officer for LADOT, Marcel Porras, specified what the city would use the program for.<sup>217</sup> He said that they would look at a map of the city, see where the mobility devices are, and require the companies to move them around to make the city more balanced.<sup>218</sup> Controlling the location of the e-scooters and other forms of mobile transportation could also benefit lower income areas by requiring the scooter companies to redistribute the scooters or bikes to underserved areas.<sup>219</sup> The program would also be able to identify abandoned mobility devices that have been in the same location for longer than five days.<sup>220</sup>

The officials who developed the Mobility Data Specification said that they specifically designed the program to not be limited to tracking scooters, but also capable of tracking other forms of transportation like Uber and Lyft in the future.<sup>221</sup> The producers of the MDS were looking forward to potential future issues including “autonomous vehicles” and “delivery drones.”<sup>222</sup> Reynolds said on behalf of the LADOT that “our job is to move people and goods as quickly and

---

<sup>213</sup> Christopher Carey, *How Los Angeles took control of its mobility data*, CITIES TODAY (July 1, 2020), <https://cities-today.com/how-los-angeles-took-control-of-its-mobility-data/>.

<sup>214</sup> See *supra* section V.

<sup>215</sup> *The Future of Mobility*, OPEN MOBILITY FOUNDATION, <https://www.openmobilityfoundation.org/> (last visited Feb. 23, 2020).

<sup>216</sup> *Id.*

<sup>217</sup> Nordrum, *supra* note 74.

<sup>218</sup> *Id.*

<sup>219</sup> Andrew J. Hawkins, *New startup aims to bring controversial scooter tracking system to more cities*, THE VERGE (Sep. 23, 2019, 10:00 AM), <https://www.theverge.com/2019/9/23/20872421/lacuna-startup-mds-scooter-tracking-ladot-data-collection>.

<sup>220</sup> Nordrum, *supra* note 74.

<sup>221</sup> *Id.*

<sup>222</sup> Bliss, *supra* note 203.

safely as possible, but we can only do that if we have a complete picture of what's on our streets and where."<sup>223</sup>

It is uncontested that this program would have benefits. If a city is able to organize where different forms of mobility are, and make sure they are where they need to be, as described above, the city will clearly have more control and be able to run the city more efficiently. However, as discussed above, there are privacy concerns. Are these benefits enough to outweigh the privacy concerns that have been raised? And how big of an issue really are the concerns that have been raised? This brings us to the main question of this entire article: how does the location tracking relate to the Constitution?

## X. HOW DOES THE REQUIREMENT TO PROVIDE DATA RELATE TO THE FOURTH AMENDMENT

In order to understand how requiring mobility companies to turn over location data in order to receive an operating permit has anything to do with the Constitution and the Fourth Amendment, we must refer back to the case law that was discussed in the beginning of this article,<sup>224</sup> and compare it to the issue at hand.<sup>225</sup>

As stated, the Fourth Amendment has several requirements that must be fulfilled before it is implicated to protect any individual.<sup>226</sup> The first requirement is that the individual seeking protection from the alleged violation must have sufficient connection with the country.<sup>227</sup> This article will assume, *arguendo*, that at least some of the e-scooter riders are United States citizens who the Fourth Amendment protects.<sup>228</sup> Therefore, the first requirement for the Fourth Amendment's protection is fulfilled.

The next requirement is that a government entity conduct the surveillance.<sup>229</sup> This is where the first issue arises. At first glance it appears that *private* mobility companies are collecting data from the users.<sup>230</sup> If that was the entire story, then we would not have a Fourth Amendment issue; however, the details are important. Here, it is more than just the private companies collecting data.<sup>231</sup>

---

<sup>223</sup> *Id.*

<sup>224</sup> *See supra* sections I and II.

<sup>225</sup> *See supra* section III.

<sup>226</sup> *See supra* sections I and II.

<sup>227</sup> *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1989).

<sup>228</sup> Micah Toll, *The results are in and Americans are loving electric scooter share programs*, ELECTREK (Aug. 14, 2018, 8:59 AM), <https://electrek.co/2018/08/14/americans-love-electric-scooter-shares/> (presenting survey information that 72% of Americans had used a scooter share program); Populus, *The Micro-Mobility Revolution: The Introduction and Adoption of Electric Scooters in the United States*, TRANSPORTATION RESEARCH BOARD (Jul. 30, 2018 9:16 AM) [https://www.populus.ai/micro-mobility-2018-july\\_](https://www.populus.ai/micro-mobility-2018-july_) (studying electric scooter usage and finding an average adoption rate of 3.6% across major cities, as measured by the percentage of people who have ever used these services).

<sup>229</sup> *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921).

<sup>230</sup> Ng, *supra* note 82.

<sup>231</sup> *Id.*

As discussed above, the Fourth Amendment can control a private entity if there are certain situations in place to convert the private action into state action.<sup>232</sup> In order for a private company's action to become state action, the government must strongly encourage the action, or it has to be a requirement of a regulatory regime.<sup>233</sup> In *Skinner*, a law that strongly encouraged a company to drug test employees converted the private action into state action.<sup>234</sup>

Comparing *Skinner* to the circumstances at hand makes it clear that the private action from the mobility companies has converted to state action. Here, the cities using MDS require companies who want to place their products within the city limits provide location data in order to obtain an operating permit.<sup>235</sup> This regulation mandating the companies to turn over data in order to have an operating permit creates a regulatory regime, thus turning the private action into state action.

Therefore, since the users of the scooters have Fourth Amendment rights that can be violated, and since the act of recording data becomes state action via the government mandate, it seems that this would implicate the Fourth Amendment. However, even if there are Fourth Amendment implications because it is state action and the person has sufficient connections, some situations simply will never violate the Fourth Amendment.<sup>236</sup> In order for the Fourth Amendment to apply, there must be a search which violates the individual's reasonable expectation of privacy.<sup>237</sup>

One of the situations that will usually never violate the Fourth Amendment is when the person under surveillance is in public.<sup>238</sup> Comparing that to the case at hand, we again seem to run into a roadblock. The Mobility Data Specification wants to collect anonymous route data, including where a scooter trip started and where it ended.<sup>239</sup> Therefore, the data the MDS collects only contains information about the person when they are in public. In *Knotts*, the government tracked movement on a public road, and this was not considered a search that violated the Fourth Amendment.<sup>240</sup> So it would seem that the tracking is not an issue, and that the cities that use the MDS are free to collect the data, since it is in public. However, there is another level to analyze.

While the movement may be in public, there are more privacy issues that are not immediately apparent. A search occurs when a person's reasonable expectation of privacy is violated by government intrusion.<sup>241</sup> *Carpenter* helps to understand what a reasonable expectation of privacy is in the context of the

---

<sup>232</sup> *Skinner v. Ry. Labor Exec.s' Ass'n*, 489 U.S. 602, 614–16 (1989).

<sup>233</sup> *Id.*

<sup>234</sup> *Id.*

<sup>235</sup> Ng, *supra* note 82.

<sup>236</sup> *See, e.g., supra* section II.

<sup>237</sup> *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018).

<sup>238</sup> *United States v. Knotts*, 460 U.S. 276, 281–86 (1983) (holding that tracking on public roads does not constitute surveillance).

<sup>239</sup> Ng, *supra* note 82; Eric Garcetti, *LADOT Data Protection Principles*, DEPARTMENT OF TRANSPORTATION, 2 (April 12, 2019) [https://ladot.io/wp-content/uploads/2019/03/2019-04-12\\_Data-Protection-Principles.pdf](https://ladot.io/wp-content/uploads/2019/03/2019-04-12_Data-Protection-Principles.pdf).

<sup>240</sup> *Knotts*, 460 U.S. at 281–82.

<sup>241</sup> *Carpenter*, 138 S. Ct. at 2214.

circumstances at hand. In that case, the Court found that tracking an individual's movements with their cell phone records violated a person's reasonable expectation of privacy.<sup>242</sup> Further, it did not matter that the movements they tracked were movements that occurred in a public place.<sup>243</sup> This was an issue because the level of detail about the person that the tracking showed and the duration of time that the government could tell where the person was.<sup>244</sup>

A second case described above that should also be taken into account is *Jones*.<sup>245</sup> As discussed, the concurrence in *Jones* discussed how tracking people, even if it is in public, could disclose information about them that violates their reasonable expectation of privacy.<sup>246</sup> The concurrence reached this conclusion because knowing the person's location over a long period of time would disclose intimate information that the Fourth Amendment tries to protect,<sup>247</sup> such as religious information, sexual or familial association, or political associations.<sup>248</sup> Since these details are so private, even tracking on public roads could be a violation of a person's reasonable expectation of privacy.<sup>249</sup>

This concept of revealing intimate information is what causes issues in the circumstances at hand with the e-scooter tracking. The scooter rides will all be on public roads, and since the cities want the companies to collect start and end points and route data, the location data will all be information that is in public view.<sup>250</sup> This does not mean there are no issues, however; just like in *Jones* and *Carpenter*, whoever holds the information about the trips, could discover intimate details about the individual rider's life, just like the Electronic Frontier Foundation<sup>251</sup> and the Center for Democracy and Technology<sup>252</sup> are concerned with.<sup>253</sup> The scooter rider would be subject to the government knowing intimate details about their daily lives, including information about their religious, sexual, familial, and political life.

It does not matter that the companies anonymize the location data by removing names, since realistically, even with anonymous data, the holder can

---

<sup>242</sup> *Id.* at 2216–17.

<sup>243</sup> *Id.*

<sup>244</sup> *Id.*

<sup>245</sup> *United States v. Jones*, 656 U.S. 400, 402 (2012).

<sup>246</sup> *Id.* at 418–31.

<sup>247</sup> *Id.*

<sup>248</sup> *Id.*

<sup>249</sup> *Id.*; *Carpenter*, 138 S. Ct. at 2217–18.

<sup>250</sup> Ng, *supra* note 82.

<sup>251</sup> Letter from Jamie Williams, et al., ELECTRONIC FRONTIER FOUND., to Mike Bonin, L.A. CITY COUNCIL, regarding *Urgent Concerns Regarding the Lack of Privacy Protections for Sensitive Personal Data Collected Via LADOT's Mobility Data Specification* (April 3, 2019), [https://www.eff.org/files/2019/04/03/eff\\_oti\\_letter\\_re\\_ladot\\_mds\\_privacy\\_concerns\\_april\\_3\\_2019.pdf](https://www.eff.org/files/2019/04/03/eff_oti_letter_re_ladot_mds_privacy_concerns_april_3_2019.pdf).

<sup>252</sup> Email from Gregory Nojeim, et al., THE CTR. FOR DEMOCRACY AND TECH., to Jeff Marootian

DIST. DEPT. OF TRANSP., regarding *Urgent Privacy Concerns With City's Decision To Collect Traveler Mobility Location Information*, (Mar. 20, 2020) <https://cdt.org/wp-content/uploads/2020/03/2020-03-20-CDT-Letters-to-DDOT-LADOT-regarding-mobility-data.pdf>.

<sup>253</sup> Torchinsky, *supra* note 70; Williams, *supra* note 127.

still identify the person who is making the trips with a high level of accuracy.<sup>254</sup> So if the information is turned over to the government, it is an invasion of a person's reasonable expectation of privacy if a court were to follow the guidelines of *Carpenter* and *Jones*.

Proponents of the MDS may argue that it only requires the mobility companies to turn over the information to the *cities* who want to manage this information so they can organize their streets.<sup>255</sup> It does not require that the data be given to law enforcement agencies, and that data will only be given to law enforcement when there is a proper court order.<sup>256</sup> Those proponents may argue that this information is harmless and would not have any criminal implications. This argument is also similar to the argument that the LADOT made for why the CalECPA did not apply to limit the cities from collecting the data.<sup>257</sup> However, in response to this argument, we must refer back to the Fourth Amendment, and the case law that clarifies it.<sup>258</sup> The Fourth Amendment is not written explicitly to apply to only law enforcement, like CalECPA; instead, it applies to the government broadly.<sup>259</sup> To reiterate, when the *government* conducts surveillance that infringes on a person's reasonable expectation of privacy, there is a violation of the Fourth Amendment.<sup>260</sup> Therefore, it does not matter that the city governments are only disclosing the information to law enforcement agencies after they have a proper court order;<sup>261</sup> the Fourth Amendment is still in play when any type of government entity is conducting surveillance,<sup>262</sup> and that seems to be implicated in this case. Keep in mind that the regulatory regime put in place by the various cities has converted the private action from the mobility companies to state action.<sup>263</sup>

## XI. SUGGESTIONS TO AVOID THE ISSUE

It is clear that as the population continues to grow, and more technology is developed, cities will become busier and more congested, and there may be some need to organize the congestion to keep it manageable, just like the cities claim.<sup>264</sup> This is a valid concern. But at the same time, there is a competing interest of citizen's rights to be free from government intrusion into their intimate lives.<sup>265</sup> A

<sup>254</sup> Valentino-Devries, et al., *supra* note 159; de Montjoye, et al., *supra* note 170.

<sup>255</sup> Marshall, *supra* note 64; Garcetti, *supra* note 239.

<sup>256</sup> Marshall, *supra* note 67.

<sup>257</sup> *See supra*, note 204; Letter from Seleta Reynolds, DEPT. OF TRANSP., to Mike Bonin, L.A. CITY COUNCIL, *STATE OFFICE OF LEGISLATIVE COUNSEL OPINION ON THE CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT* (Aug. 15, 2019), [https://cdn.theatlantic.com/assets/media/files/17-1125-s8\\_rpt\\_dot\\_08-15-2019.pdf](https://cdn.theatlantic.com/assets/media/files/17-1125-s8_rpt_dot_08-15-2019.pdf).

<sup>258</sup> *See supra*, section I and II.

<sup>259</sup> *See supra*, section I and II.

<sup>260</sup> *See supra*, section I and II.

<sup>261</sup> *See Ng, supra* note 82.

<sup>262</sup> *See, e.g., Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018); *Skinner v. Ry. Labor Exec.s' Ass'n*, 489 U.S. 602, 614–16 (1989); *United States v. Knotts*, 460 U.S. 276, 281–86 (1983).

<sup>263</sup> *Skinner*, 489 U.S. at 614–16.

<sup>264</sup> *See supra*, section VIII.

<sup>265</sup> U.S. CONST. amend. IV.

balance must be found between these two valid and important interests. As Uber and other mobility companies have made clear, they are willing to work with the cities to reach the goals, as long as they can protect their rider's privacy.<sup>266</sup>

Cities should not ignore these offers to negotiate or other opportunities to come to a creative solution. One potential solution which would still serve the cities' interests and also protect the rider's privacy is to simply share the end location of the scooter after the trip is done with no connection to any personal information of the user. This data should be raw location data and not include any PII or UDID information which can create privacy issues.<sup>267</sup> That way, the city would still be able to see where the scooters are, but would not have the real time data, nor any connection to the users of the scooters. Admittedly, this would not let the cities know where all scooters are at all times as they have wanted, but this would be a good compromise between the two sides.

Even more beneficial to the rider's privacy, the cities could take a hands-off approach and simply allow the mobility companies to manage their fleets in an efficient manner. Because of the city planning and organization concerns, this is less likely. But the government cannot invade the constitutional privacy rights of its citizens on its path to city organization.

## XII. CONCLUSION

As the world changes, and more technologies develop, courts have struggled to keep up. However, they have always maintained a consistent attitude of enforcing citizens' constitutional protections. This is another issue that courts will be grappling with in years to come. The lawsuits by Uber, the ACLU, and the EFF against the LADOT show that privacy is not something to be taken lightly. It is likely that there will be more litigation, and more issues that arise as the governments try to push for more data. As Jamie Williams, a staff attorney for the Electronic Frontier Foundation said, "Just looking at scooter data is too short sighted – this is a model for getting access to data for other transportation ... Scooters are a really divisive issue, but a lot of those people also probably taking Lyft and Uber and would feel differently about that data."<sup>268</sup> Cities have an interest in organizing their streets, but citizens have a fundamental right to privacy under the Constitution. The privacy issues must be avoided, or the pending lawsuits could turn into major clashes, or cities could infringe too far into their citizens' lives.

---

<sup>266</sup> Bliss, *supra* note 203.

<sup>267</sup> Duarte and Jerome, *supra* note 133.

<sup>268</sup> Kia Kokalitcheva, *Scooters, cities clash over rider data*, AXIOS (Jun. 29, 2019), <https://www.axios.com/scooter-companies-cities-rules-54bc7d58-e36a-487a-b4b2-3408fd41e7fe.html>.