Article

Scoot over Smart Devices: The Invisible Costs of Rental Scooters

Andrew Boyles Petersen

Michigan State University, USA
andyjp@msu.edu

Abstract

In the past year, transportation rental companies, including Bird, Lime, and Spin, have dropped hundreds of thousands of rental scooters across North America. Relying on mobile apps and scooter-mounted GPS units, these devices have access to a wide-variety of consumer data, including location, phone number, phone metadata, and more. Pairing corroborated phone and scooter GPS data with a last-mile transportation business model, scooter companies are able to collect a unique, highly identifying dataset on users. Data collected by these companies can be utilized by internal researchers or sold to advertisers and data brokers. Access to so much consumer data, however, poses serious security risks. Although Bird, Lime, and Spin posit electric scooters as environmentally friendly and accessible transportation, they also allow for unethical uses of user data through vaguely-worded terms of service. To promote more equitable transportation practices, this article will explore the implications of dockless scooter geotracking, as well as related infrastructure, privacy, and data security ramifications.

Introduction

In under a year, hundreds of thousands of rental scooters have been dropped across North America, deploying to over 120 locations and adding new cities and campuses on an almost monthly basis. Although the vast majority of locations have thus far been in the United States, rental scooters are steadily making inroads in Canada, Europe, and Central and South America. These scooters are dockless, with users locating and unlocking scooters through a location-enabled smartphone. Throughout their ride, the app will track their progress, saving the path of their completed trip for later viewing. Scooter-mounted GPS units and wireless connectivity pair with the app-based tracking in order to verify app-based data and paint an accurate map of a user's location.

Ostensibly, location data from scooter GPS units, data connections, and mobile apps is used to help users find scooters to rent, prevent theft, and allow companies to gather scooters for charging or service. When user location data is paired with the wealth of personally identifying information that companies require to access the scooters, however, users face serious security and surveillance risks. According to JiWire president David Staas, "Where you are says more about you than any other point of data," and when compiled with other information, location data provides an exceedingly accurate portrait of an individuals' social connections and preferences (Angwin 2015: 149). Although Bird, Lime, and Spin posit their electric scooters as environmentally friendly and accessible transportation, they also allow for unethical uses of user data through location tracking and extensive collection of personal information. Relying on loosely worded terms of service and privacy policies, these companies reserve the right to monetize customer data, allowing

Petersen, Andrew Boyles. 2019. Scoot over Smart Devices: The Invisible Costs of Rental Scooters. *Surveillance & Society* 17(1/2): 191-197.

<https://ojs.library.queensu.ca/index.php/surveillance-and-society/index> | ISSN: 1477-7487

© The author(s), 2019 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](#)

for sharing with governments and third parties. Since scooter companies have access to more accurate and authenticated door-to-door data than other ride sharing platforms, they pose a more significant threat to users. By analyzing scooter company policies and public statements, as well as the actions of similar gig economy corporations, this article will explore the risks and repercussions of trusting scooter rental companies with consumer data and will make recommendations for better data stewardship and improved privacy practices.

Our Data Rights: A History

Although scooter rental companies posit the collection of location data is solely for finding, using, and servicing scooters, research shows that much more can be done with these sorts of data. In 1999, the United States Federal Communications Commission sought to improve emergency services, laying out new parameters for 911 emergency calls and mandating wireless network providers supply emergency services with the phone number and “call location information concerning the user of a commercial mobile service” (Wireless Communications and Public Safety Act of 1999, 1999). Initially, call location information focused predominantly on network-based cell tower connections, triangulating signals between cell towers. In 2000, Bolla and Davoli (2000) presented an innovative use of network-based locational data, proposing using cellular data connections to estimate traffic conditions on high-use roadways. By using location data similar to that provided to emergency services, the team suggested that real-time traffic data, including vehicle speed, slowdowns, and traffic density, could be predicted. Research on location data usage for traffic prediction steadily grew, with Cayford and Johnson (2003) suggesting the effectiveness of using cellular data for traffic monitoring is dependent on location accuracy, frequency of location updates, and number of locations able to monitor traffic data.

In addition to roadway-specific traffic analysis, cellular location data began being heavily used for the prediction of travel patterns through origin-destination (OD) matrices. OD matrices are used to measure transportation patterns, using a matrix to analyze the number of trips from each origin to destination. Traditionally, OD matrices in traffic prediction had been largely reliant on surveys or traffic counting and monitoring devices, both of which were expensive, time-consuming, and limited in their scope (Zhang et al. 2010). However, as wireless network providers and mobile phone manufacturers shifted to location capable phones in order to comply with the 1999 FCC mandates, researchers had a new opportunity of accessing large, accurate, regularly updated location data sets. These data sets were additionally supplemented when manufactures began installing Global Positioning System (GPS) receivers, complementing the network-based cellular location information previously used. Through network-based and GPS location data sets, mobile phone networks could be used to create origin-destination matrices independent of traditional traffic prediction methods (Caracas, Wideberg, and Benitez 2007; Calabrese et al. 2011).

Branching away from using location information for transportation analysis, companies and researchers began using location data to predict social ties, aid in urban planning, and develop consumer profiles for targeted marketing. For all of these uses, mobile phone location data provided “new opportunities to examine individual mobility with their lower collection costs, larger sample sizes, higher update frequencies, and a broader spatial and temporal coverage...” (Malleson et al. 2018). With access to location data, massive amounts of information can be determined about individuals’ habits. Even when relying on selective location data—specifically users opting to geo-tag photos—Crandall et al. (2010) were able to demonstrate high probability of social connections through co-occurrences of user location data. Their findings suggest that companies with access to more robust data sets can infer even more personal details about users. In 2011, German politician Malte Spitz proved these findings when he sued Deutsche Telekom—his telecommunications provider—for access to the data they had collected from his mobile phone between August 2009 and February 2010. Spitz and the publication *Zeit* then created an analysis of these data, overlaying location data with other publicly available information, including his social media posts and blog entries (Biermann 2011). This pairing provided an inordinate amount of information on Spitz,

including his movements, relationships, food and shopping preferences. Ultimately, “it reveals an entire life” (Biermann 2011).

Location Data in the Gig Economy

Many gig economy platforms have become heavily dependent on location data, utilizing network-based and GPS location data to surveil their workforce and clientele. Services ranging from dog walkers, ride sharing platforms, courier services, and home cleaners collect location data, ostensibly using it to track workers and provide updates to customers. In the short term this can be convenient, providing an accurate map of where a dogwalker went with your pet or predicting how far away an Uber or Lyft driver is. With these companies often arguing they only provide a service platform—not the actual service—collection of location data allows them to distance themselves from the individuals performing a service. Through live-tracking and collection of location data, the company can shift responsibility for the success of a task to the employees and customers by suggesting the platform is correctly facilitating the service. This provides the company with a guarantee that workers are performing a service and additionally provides the employees a modicum of proof they are completing a task. This model shifts responsibility for labor from the service while simultaneously giving them rights to an exorbitant amount of their employee’s and client’s personal data. Multiple high-profile recent misuses of gig economy location data reveal that corporations often aren’t responsible stewards of this information, taking opportunities to profit from and manipulate these data for their own gain (Voytek 2012; Fung 2017).

To consider the problematic uses of location data for scooter rental providers, it’s important to look at their similarities to other gig economy companies. At present, Uber, Lyft, and similar ride sharing platforms are the most comparable corporations to scooter rental companies, providing us a unique example for analyzing location data collection and misuse. In North America, ride sharing platforms provide transportation services, are part of the gig economy, are targeted to similar audiences as scooters, and are used in largely similar ways. Ride sharing platforms are predominantly geared towards higher-income brackets and younger audiences, and these services are generally used for in-town transportation, particularly in or around urban areas (Smith 2016). Collecting similar location data to scooter rental companies—namely GPS and network-based location data—usage of ride sharing platforms can reveal a user’s personal relationships, hobbies, employment, and other connections.

Of the various ride sharing platforms, Uber has particularly demonstrated the risks associated with trusting for-profit companies with user location data. One crucial aspect of user data stewardship is robust information security, including both regulation of internal access to user data and safeguards to protect those data from outside breaches. On multiple occasions, Uber has taken a cavalier approach to protecting user data in its advertising and software development. In 2012, Uber published a much-maligned blog post titled “Rides of Glory.” This post created a data set of one-night stands, mapping riders that used Uber on a weekend night, then took an additional ride from near the same drop-off point early the next morning (Voytek 2012). With this data set, Uber temporally and locationally analyzed its perceived customer hookups, mapping behavior by gender, neighborhood, and day of the year. Alongside concerns over Uber’s voyeuristic analyses, this post helped point out that “tracking an Uber user’s ride history can unearth where they live, where they work, who they hang out with and, yes, maybe even who they’re sleeping with... It’s a data set with particularly terrifying privacy repercussions” (Sobel Fitts 2015).

Outside of its blog posts, Uber has misused location data in the construction and use of multiple internal software programs. In the wake of a massive 2014 data breach in which over 38 million Uber employees’ and customers’ personal information—including driver trip summaries—were released, Uber reached settlements with both the US Federal Trade Commission (FTC) and European authorities (Fung 2017; Hern 2018). As part of this settlement, the FTC expressed concern over Uber’s misuse of a program alternately known as “God View” and “Heaven.” This program provided Uber corporate employees with real-time monitoring of driver and customer locations and routes (Fung 2017). Uber employees used the program to track investigative journalists; display user locations to attendees of corporate parties; or allegedly, to follow

the whereabouts of politicians, celebrities, and ex-partners (Osborne 2016; Spangenberg 2016). In addition to misusing the “God View” program, the 2017 FTC settlement noted Uber stored unencrypted customer information and location data online and failed to implement basic data security practices such as two-factor authentication.

Such blatant mishandling of personal data can have horrifying repercussions, including identity theft, threats to personal security, public embarrassment, censorship, and surveillance. The risk of governmental surveillance came to the forefront in 2017 when the Egyptian government requested Uber provide real-time access to its Heaven software. Although the final draft of an Egyptian bill regulating ride sharing companies doesn’t require constant, real-time access, it does mandate Uber “retain user data for 180 days and share it with authorities ‘on request’ and ‘according to the law’” (Hamdi, Mourad, and Knecht 2018). With these provisions and Uber’s loose standards, this law could provide authorities with the locations and social networks of activists, dissidents, and rival politicians, limiting free speech and supporting autocratic rule.

Scooter Surveillance

With an even more invasive user data collection structure than Uber and other ride sharing companies, the surveillance risks associated with scooter rental transportation companies like Bird, Lime, and Spin are highly concerning. Like Uber’s tracking of user locations, scooter rental companies’ apps rely on network-based and GPS location data collected from users’ smartphones. Diverging from the data collection of ride share companies, scooters are able to collect the perfect cocktail of user data, gathering multi-source verified information through both scooters and apps. Unlike ride share services, scooter companies posit themselves as last-mile transportation, gaining an even more accurate picture of a user’s commute. Beginning when users open the app to search for a scooter, these apps can track where individuals ride, possibly revealing users’ living arrangements, employment, social connections, and consumer behavior. On the off chance users disable location tracking on their phone after unlocking a scooter, each scooter has location tracking capabilities built in through GPS chips and 4G data connections. When pairing scooter location data with that from a users’ phone, each data set can be corroborated, providing an exceptionally accurate portrait of a users’ location and trip routes. Over time, these trip routes can paint a clear picture of a users’ lifestyle and preferences.

This multi-source verification also makes scooter surveillance more concerning than ride sharing services and poses significant risks to users. On initial deployment, most of these companies had policies enabling them to collect and share user data with other companies and when lawfully required. In these policies, collected user data includes name, e-mail address, telephone number, postal address, demographic information, credit card, billing and contact information, demographic information, and location information (Lime 2018; Bird Rides, Inc. 2018; Skinny Labs Inc. 2018). In addition to the bulk collection of these data, companies “may combine information gathered from multiple portions of the services into a single customer record or analysis or report” (Bird Rides, Inc. 2018). With these aggregated data, an extraordinarily accurate profile of a user can be assembled, opening a concerning possibility of user surveillance. As with Malte Spitz’s phone data, “seen individually, the pieces of data are mostly inconsequential and harmless. But taken together, they provide what investigators call a profile—a clear picture of a person’s habits and preferences, and indeed of his or her life” (Biermann 2011).

Although each company provides an ability to opt-out of data collection, Spin’s privacy policy describes these opt-out clauses best by stating, “If you do not want information about you to be used in the manner set forth in this policy, the services may not be fully available to you” (Skinny Labs Inc. 2018). Without enabling phone location data, the services’ apps are unable to locate and unlock scooters, rendering them unusable. Likewise, these apps are required to activate a scooter, linking the user to that scooter’s location tracking system. Even with the protection or separation of a user’s data, this location information could be used to determine their identity, as well as predict their movements. Companies do not need to compile and retain this information to successfully run a business; however, requiring it forces users into an unnecessary tradeoff—either give away their data in exchange for convenience or choose not to use a service at all. By

retaining the right to compile and store user data, companies are able to ensure they have a potential avenue for profit in the future, particularly when they “reserve the right to amend [privacy policies] at any time...” (Bird Rides, Inc. 2018).

After reaching out to Bird, Lime, and Spin, all three companies declined to comment on their use of location data and information security practices for this publication. Nevertheless, we can gather some information about these company’s practices based on previous public comments and analysis of their terms of service and privacy policies. At present, some companies are taking a firm stance on their usage of user data without taking steps to lend credence to this assurance. Although Bird has stated that “we will never advertise on the birds and we would never share or sell customer data or anything silly like that,” their privacy policy and terms of service leave open the possibility of doing exactly that (Nikolewski 2018). In their current privacy policy, Bird lists that data can be shared with business partners, sponsors, unnamed third parties, third-party service providers, and in emergency or legal situations, governments or law enforcement (Bird Rides, Inc. 2018). Put more directly, in April 2018, a representative from Lime stated that they were “exploring other revenue streams through partnerships, whether its advertising or partnering with other private companies. But right now because ridership is actually quite high, we’re able to run a sustainable business” (Nikolewski 2018). With Bird and Lime’s January 2019 valuations coming in lower than expected, the possibility of monetizing user data may be closer than expected (Newcomer 2019).

Ambiguous privacy practices pose a strong risk to marginalized communities and a high likelihood of monetization. As scooters provide a relatively inexpensive, convenient, and accessible transportation source, they could be relied upon by low-income individuals. Being both cheaper than ride-share alternatives and an accessible way to escape redlining, it is unsurprising surveys of users find a statistically higher percentage of individuals below the poverty line optimistic about electric scooters (Populus Technologies, Inc. 2018). Moreover, Bird, Lime, and Spin all offer discount programs to encourage usage by marginalized individuals. These two factors demonstrate a clear risk to marginalized and transportation vulnerable communities. User data and activity logs could be turned over to police, mental health professionals, and insurance companies to raise rates, reinforce redlining, and/or encourage harassment. As the North American political climate becomes increasingly volatile, the likelihood of such activity only increases. With scooter companies already offering up data to local governments in hopes of securing future business contracts, it is only a matter of time before these data are increasingly misused or monetized (Marshall 2018).

Possible Solutions

To help prevent such misuse of personal data and protect user privacy, scooter rental companies need to take strong steps towards addressing security and surveillance risks. One strategy is to implement comprehensive security plans; as the American Civil Liberties Union Foundation of Northern California notes:

Bird, Lime, and Spin also seem to have zoomed past developing a comprehensive security plan and communicating it to users. All three vow to secure your most sensitive data, including your financial data, but it’s not clear what precautions they actually take. Spin tells users about any internal data security policies, makes a vague reference to “bank level security” in its app, and highlights some data breach procedures, but these half measures are inadequate. Bird and Lime are silent on security matters and also explicitly reserve the right to transfer data to other jurisdictions that may not be governed by U.S. law. None of this is a good signal to send to people about privacy and data security. (Conway 2018)

Comprehensive security plans involve strongly considering issues of privacy and security by taking steps to limit internal and external access to data, to secure and encrypt data, and to communicate effectively with users regarding privacy issues. With these policies, companies can communicate what data are collected,

how they can be used, and how long they are retained. Implementing data stewardship practices focused on equity and sustainability will aid scooter rental companies both in developing an ethical business model and in gaining the public trust. One key step towards this goal would be increasing transparency by making informed, ethical, and permanent policies regarding data stewardship practices.

Another crucial strategy would be to allow users to opt-out of data tracking while still utilizing scooter services. Even if these users' location information is used to help facilitate transportation, it does not need to be retained. A rider's usage information could be recorded during a trip, and upon completion of the ride or nightly reacquisition of the scooter for charging, the use information could be erased. Similar models are in play in other successful businesses, such as the search engine DuckDuckGo or the email service ProtonMail. This would prevent unethical uses of client information, particularly the bulk compilation of a user's location data, and would provide better data protection for customers. Additionally, improving the data stewardship practices of scooter rental companies and other gig economy enterprises requires the implementation of effective laws and regulations. As stated by Bruce Schneier, "law and policy may not seem as cool as digital tech, but they're also places of critical innovation. They're where we collectively bring about the world we want to live in" (Schneier 2017).

Changing our data privacy practices is necessary in our increasingly technological world. Being more conscientious about our data privacy policies affirms the values of our material culture in the digital age, particularly through the valuation of privacy, security, and equality for all people. If we fail to uphold these values, we risk exacerbating the unethical treatment of marginalized individuals. As such, it is crucial that we uphold the social safety net and build the infrastructure for a world we all want to live in. One first step is to hold companies accountable for their stewardship of user data. Only when we take action against providing companies with unfettered access to our lives can we bring about a world of innovation and equality.

References

- Angwin, Julia. 2015. *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York: St. Martin's Press.
- Biermann, Kai. 2011. Data Protection: Betrayed by Our Own Data. *Die Zeit* (Hamburg, Germany), March 10. Accessed December 1, 2018. <https://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz>.
- Bird Rides, Inc. 2018. Privacy Policy. Bird. Accessed December 1, 2018. <https://www.bird.co/privacy/>.
- Bolla, Raffaele, and Franco Davoli. 2000. Road Traffic Estimation from Location Tracking Data in the Mobile Cellular Network. *IEEE Wireless Communications and Networking Conference* 3: 1107-12. <https://doi.org/10.1109/WCNC.2000.904783>.
- Calabrese, Francesco, Giusy Di Lorenzo, Liang Liu, and Carlo Ratti. 2011. Estimating Origin-Destination Flows Using Mobile Phone Location Data. *IEEE Pervasive Computing* 10(4): 36-44. <https://doi.org/10.1109/MPRV.2011.41>.
- Caraces, N., J.P. Wideberg, and F.G. Benitez. 2007. Deriving Origin Destination Data from a Mobile Phone Network. *IET Intelligent Transport Systems* 1(1): 15-26. <https://doi.org/10.1049/iet-its:20060020>.
- Cayford, Randall, and Tigran Johnson. 2003. Operational Parameters Affecting the Use of Anonymous Cell Phone Tracking for Generating Traffic Information. *Transportation Research Board 82nd Annual Meeting*. Accessed December 1, 2018. <https://trid.trb.org/view/645521>.
- Conway, Nomi. 2018. Electric Scooters Are Racing to Collect Your Data. *ACLU Northern California* (blog). Entry posted July 25, 2018. Accessed December 1, 2018. <https://www.aclunc.org/blog/electric-scooters-are-racing-collect-your-data>.
- Crandall, Daniel, Lars Backstrom, Siddharth Suri, Daniel Huttenlocher, and Jon Kleinberg. 2010. Inferring Social Ties from Geographic Coincidences. *Proceedings of the National Academy of Sciences* 107(52): 22436-41. <https://doi.org/10.1073/pnas.1006155107>.
- Fung, Brian. 2017. Uber Settles with FTC over 'God View' and Some Other Privacy Issues. *Los Angeles Times* (Los Angeles, CA), August 15. Accessed December 1, 2018. <https://www.latimes.com/business/technology/la-fi-tn-uber-ftc-20170815-story.html>.
- Hamdi, Nashaat, Mahmoud Mourad, and Eric Knecht. 2018. Egypt Passes Law Regulating Uber, Careem Ride-Sharing Services. *Reuters*, May 7, Technology News. Accessed December 1, 2018. <https://www.reuters.com/article/us-egypt-uber-idUSKBN1I81VG>.
- Hern, Alex. 2018. Uber Fined £385,000 for Data Breach Affecting Millions of Passengers. *The Guardian* (London, United Kingdom), November 27, Technology. Accessed December 1, 2018. <https://www.theguardian.com/technology/2018/nov/27/uber-fined-385000-for-data-breach-affecting-millions-of-passengers-hacked>.
- Lime. 2018. Privacy Notice. Lime. Accessed December 1, 2018. https://www.li.me/privacy#privacy_21.

- Malleon, Nick, Anthony Vanky, Behrooz Hashemian, Paolo Santi, Santosh Verma, Theodore Courtney, and Carlo Ratti. 2018. The Characteristics of Asymmetric Pedestrian Behavior: A Preliminary Study Using Passive Smartphone Location Data. *Transactions in GIS* 22(2): 618-634.
- Marshall, Aarian. 2018. Still smarting from Uber, cities wise up about scooter data. *Wired*, September 18, 2018. Accessed January 31, 2019. <https://www.wired.com/story/cities-scooter-data-remix-uber-lyft/>.
- Newcomer, Eric. 2019. Lime and Bird raise millions, but at far lower valuations than hoped. *Bloomberg News*, January 17. Accessed January 31, 2019. <https://www.bloomberg.com/news/articles/2019-01-17/lime-bird-said-to-raise-millions-at-lower-valuations-than-hoped>.
- Nikolewski, Rob. 2018. How Can Dockless Bike and Scooter Companies Make Money? *The San Diego Union-Tribune* (San Diego, CA), April 15. Accessed December 1, 2018. <https://www.sandiegouniontribune.com/business/energy-green/sd-fi-dockless-profitable-20180415-story.html>.
- Osborne, Charlie. 2016. Uber Fined \$20K in Data Breach, ‘God View’ Probe. *CNET*, January 7. Accessed December 1, 2018. <https://www.cnet.com/news/uber-fined-20k-in-surveillance-data-breach-probe/>.
- Populus Technologies, Inc. 2018. The micro-mobility revolution: The introduction and adoption of electric scooters in the United States. News release. July. Accessed January 31, 2019. https://research.populus.ai/reports/Populus_MicroMobility_2018_Jul.pdf.
- Spangenberg, Samuel Ward. 2016. Samuel Ward Spangenberg v. Uber Technologies, Inc., No. CGC-16-552156 (Superior Court of the State of California Oct. 19, 2016). Accessed December 1, 2018. <https://assets.documentcloud.org/documents/3227535/Spangenberg-Declaration.pdf>.
- Schneier, Bruce. 2017. Security and the Internet of Things. *Schneier on Security* (blog). Entry posted February 1. Accessed December 1, 2018. https://www.schneier.com/blog/archives/2017/02/security_and_th.html.
- Skinny Labs Inc. 2018. Spin Privacy Policy. Spin. Accessed December 1, 2018. <https://www.spin.app/privacy>.
- Smith, Aaron. 2016. *Shared, Collaborative, and On Demand: The New Digital Economy*. May 19. Accessed December 1, 2018. http://www.pewresearch.org/wp-content/uploads/sites/9/2016/05/PI_2016.05.19_Sharing-Economy_FINAL.pdf.
- Sobel Fitts, Alexis. 2015. Can Uber Keep Your Data Safe? It’s Trying. *Huffington Post*, August 18, Tech. Accessed December 1, 2018. https://www.huffingtonpost.com/entry/uber-data-security_us_55d230b7e4b07addcb43a7d8.
- Voytek. 2012. Rides of Glory. *Uber Blog*. March 26. Accessed December 1, 2018. <https://web.archive.org/web/20141118192805/http://blog.uber.com/ridesofglory>.
- Wireless Communication and Public Safety Act of 1999, Pub. L. No. 106-81, Stat. 4 (Oct. 26, 1999). Accessed December 1, 2018. <https://www.gpo.gov/fdsys/pkg/PLAW-106publ81/pdf/PLAW-106publ81.pdf>.
- Zhang, Yi, Xiao Qin, Shen Dong, and Bin Ran. 2010. Daily O-D Matrix Estimation Using Cellular Probe Data. *Transportation Research Board 89th Annual Meeting*, 1-20. Accessed December 1, 2018. <https://trid.trb.org/view/910539>.