**BEFORE THE PUBLIC UTILITIES COMMISSION**
**OF THE STATE OF CALIFORNIA**

| | |
|---|---|
| Order Instituting Rulemaking on Regulations Relating to Passenger Carriers, Ride Sharing, and New Online-Enabled Transportation Services | **R. 12-12-011** (Filed December 20, 2012) |

# REPLY COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION ON THE ORDER INSTITUTING RULEMAKING ON REGULATIONS RELATING TO PASSENGER CARRIERS, RIDE SHARING, AND NEW ONLINE-ENABLED TRANSPORTATION SERVICES

Lee Tien
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x 102
Facsimile: (415) 436-9993
E-Mail: tien@eff.org

Counsel for
ELECTRONIC FRONTIER FOUNDATION

Dated: February 11, 2013

## I. INTRODUCTION

The Electronic Frontier Foundation ("EFF")[1] files these reply comments pursuant to the Order Instituting Rulemaking on Regulations Relating to Passenger Carriers, Ridesharing, and New Online-Enabled Transportation Services ("OIR"). EFF understands these comments to establish party status in the proceeding without need for a separate motion.

Rideshare services may advance California policy goals such as improving transportation access, reducing greenhouse gas emissions, reducing vehicle miles traveled, and reducing traffic congestion. Nevertheless, as the Commission succinctly stated: "Businesses like Sidecar and Lyft have presented the Commission with a situation not encountered before: the use of mobile communications and social networks to connect individuals wishing to offer and receive low cost and convenient, sometimes shared, transportation. Uber likewise uses smartphones to present a different business model from traditional limousine service, by allowing passengers to use a GPS-enabled smartphone app to hail a limousine or other passenger carrier."[2]

We agree that "new technology and innovation require[] that the Commission continually review its regulation and policies."[3] Several important issues have already been identified: "exercise of [the Commission's] jurisdiction; the consumer protection and safety implications of the new methods for arranging transportation services; whether and how the new transportation business models differ from longstanding forms of ridesharing; and the new transportation business models' potential impact on insurance and transportation access."[4]

---

[1] EFF is a non-profit member-supported organization based in San Francisco, California, that works to protect free speech and privacy rights in an age of increasingly sophisticated technology Instituting Rulemaking. EFF has been active in addressing privacy issues arising in Rulemaking 08-12-009 ("Order to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System"), which led to Decision (D.) 11-07-056.

[2] OIR, at 1.

[3] OIR at 5.

[4] OIR at 10.

Absent from this list of issues, however, is the impact of new ridesharing services on consumer privacy. Consumers have a strong interest in keeping information about their trips private. In the course of offering consumers the convenience of summoning a car from their mobile devices, companies that offer this service collect much sensitive personal information, including name, phone number, age, credit card information, and GPS coordinates for a user's location during a ride, from origin to destination.

According to their privacy policies,[5] the three largest companies of this type operating in San Francisco – Uber, Lyft, and Sidecar – retain this information for as long as a user maintains an active account, perhaps longer.[6] Over time, this information can paint a detailed portrait of a user's identity and travel while using a mobile-based car service – potentially revealing sensitive information such as the user's activities and home and workplace address. If disclosed, whether intentionally or inadvertently, this sensitive information could subject one user or even thousands not just to inconvenience or embarrassment, but also to fraud or physical danger.

Detailed location information also raises concerns about law enforcement access. For example, under all three providers' current policies, law enforcement may be able to obtain what amounts to a log of users' location and activities over the course of months or even years. A recent U.S. Supreme Court case, *United States v. Jones*, 132 S. Ct. 945 (2012), highlighted the

[5] Uber, *Privacy Policy*, http://www.uber.com/legal/privacy (last visited Feb. 7, 2013) ("Uber Privacy Policy"); Lyft, *Privacy Policy*, Terms of Use, http://www.lyft.me/terms (last visited Feb. 7, 2013) ("Lyft Privacy Policy"); Sidecar, *Privacy*, Terms, http://www.side.cr/terms (last visited Feb. 7, 2013) ("Sidecar Privacy Policy").

[6] A fourth company, InstantCab, also provides both ridesharing and traditional taxicab services in San Francisco. *See* InstantCab, *Frequently Asked Questions*, http://www.instantcab.com/faq (last visited Feb. 7, 2013). Unlike its three other competitors, which make privacy policies available on their websites, InstantCab devotes only five sentences of its terms of service to privacy. Apart from referring to a privacy policy that we were unable to find, that paragraph promises only (1) not to sell or rent user information to third party advertisers without user consent and (2) to store user data in U.S.-based secure servers. *See* InstantCab, *PRIVACY*, Terms of Service, http://www.instantcab.com/terms (last visited Feb. 7, 2013).

federal constitutional privacy interest in location data by finding that police installation of a GPS tracking device on a car implicated significant Fourth Amendment privacy issues.[7]

EFF has therefore taken a strong interest in encouraging developers of mobile applications that collect user location data to properly safeguard that sensitive information. We have urged location-based mobile applications to build consumer-conscious terms into their privacy policies.[8] Crucially, the policies specified that the applications would not keep a historical log of user location data and that the developers would not disclose such data to law enforcement without a warrant.[9]

In the same spirit, the California Attorney General in January 2013 published a consumer-privacy guide for mobile application developers.[10] The guide recommends, among other things, that developers avoid collecting personal information beyond what is essential to the application's core functionality, avoid retaining sensitive data any longer than absolutely necessary, guide users to the privacy policies of third party advertisers, and give users control over the collection and use of their data.[11]

The current privacy policies of companies providing mobile app-based transportation services appear to fall short of those principles to some degree. Despite the sensitive nature of the location-based data they collect, those providers appear to store that information indefinitely – essentially maintaining a log of their users' comings and goings over the course of months or even years. The policies indicate that the companies may disclose personal user information to law enforcement and private litigants, not just when required to do so by law, but

[7] http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling/.
[8] Kevin Bankston, *EXCLUSIVE: Google Takes a Stand for Location Privacy, Along with Loopt*, Electronic Frontier Foundation (March 4, 2009), https://www.eff.org/deeplinks/2009/03/exclusive-google-takes-stand-location-privacy-alon.
[9] *Id.*
[10] California Office of the Attorney General, *Privacy On the Go: Recommendations for the Mobile Ecosystem* (Jan. 2013), *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

at the companies' "sole discretion."[12] The applications provide users little control – and in the case of one company none at all – over what data is collected about them, how that data is used and how long it is retained. And while all three services fully disclose that they share user data with third-party advertisers and allow those third parties to collect additional user data themselves, their privacy policies seem to disclaim responsibility for how such third parties collect and use customer data.

EFF believes that the Commission's consumer protection jurisdiction includes protection of consumer information privacy and security, and that this proceeding should also examine how rideshare services collect, store, safeguard and disclose information provided by or collected from users and their devices.

## II. TYPES OF INFORMATION COLLECTED

The information that mobile-based rideshare service providers collect from customers can be grouped into three broad categories. First, consumers directly provide certain information, such as name, phone number and credit card number, in order to register for an account. Second, as customers interact with these services online or through a mobile application, each provider and its third-party advertising partners also collects from users' browsers or devices data that identifies them and tracks their online activity. Finally, the providers collect and retain a history of each customer's use of the service, such as location, date, time and payment data.

### A. Personal Data Gathered During the Registration Process

Registering for an Uber, Sidecar or Lyft account requires a user to submit sensitive personal information.[13] Although the requested information varies by service, each requires at

---

[11] *Id.* at 7-13.
[12] *See*, *e.g.*, Uber Privacy Policy, *Our Disclosure of Your Information*.
[13] *See* Uber Privacy Policy, *Information We Collect*; Lyft Privacy Policy, *Data We Collect From You*; Sidecar Privacy Policy 1.

least the user's name, age, credit card number and expiration date, zip code, email address and mobile phone number. Lyft also requests a wider range of "demographic information," including the user's full postal address and gender.[14] Services like Sidecar that operate as ride-sharing services also collect vehicle registration, insurance registration and drivers license information, as well as any details necessary to complete a full background check, from users who sign up to be drivers.[15] Apart from the information required to open an account, some services also ask users to volunteer other personal content and information. For instance, Uber prompts, but does not require, users to submit a photo of themselves to help drivers identify them.[16]

Providers need much of this customer-submitted information in order to deliver the transportation service, and they use it primarily for that purpose.[17] For instance, Uber collects users' name and credit card number, expiration date and security code to bill customers, and it retains that information for expedited payment processing on future trips.[18] However, some companies also use customer-submitted personal information, internally or through third parties, for advertising, web analytics and other purposes unrelated to the service's core functionality.[19]

B. Browser and Device Information

Each time a customer interacts with a ridesharing service online or through a mobile application, the service also collects data from the user's Internet browser or mobile device about the user's identity, device and behavior. First, the services' servers automatically log certain information reported by the browser or mobile device.[20] If a browser is used, this "log file"

[14] Lyft Privacy Policy, *Data We Collect From You*.
[15] Sidecar Privacy Policy 1(1).
[16] Uber Privacy Policy, *Information We Collect*.
[17] *See*, *e.g.*, Uber, *How We Use Your Information*.
[18] *Id.*
[19] Lyft Privacy Policy, *How We Use Personal Information*.
[20] *See* Sidecar Privacy Policy 1(5).

information may include a user's web request, IP address, browser type, and data about how the user interacts with the site, including sections of the site visited, links clicked, number of clicks, and referring and exit pages.[21] Similar information is collected from a smartphone or tablet, including the device's type and universally unique identifier ("UUID").[22] Although log file data and device identifiers do not directly reveal a user's identity, the data they contain can be associated with a particular device or Internet connection and, by extension, with the person using it.[23] Providers use this information for a range of purposes that include ensuring browser compatibility, "remembering" user settings across multiple visits, aggregating demographic and site traffic data, and deliver targeted advertising.[24]

The services, directly and through third-party advertising partners, also use cookies and "clear gifs" (also known as web beacons) to track users' Internet and email usage patterns.[25] The three services' tracking policies differ. Lyft's privacy policy does not address tracking at all.[26] Uber's privacy policy suggests that it uses its own cookies and third party-provided web beacons only to recognize repeat users and to identify needed improvements to its site, but warns that Uber has no control over the use of cookies (or the information they collect) by the third-party advertising publishers it employs.[27] Sidecar uses cookies to recognize repeat users and web beacons to identify improvements to its site and email communications.[28] Its policy also warns that the collection and use of IP addresses, device UUIDs, location data, clear gifs, cookies and JavaScript by Sidecar's third-party advertising partners to track users' behavior is governed by

[21] *See id.*
[22] *See id.*
[23] *See id.* at 1(7).
[24] Sidecar Privacy Policy 1(5), (7), (10).
[25] *Id.*; Uber Privacy Policy, *Information We Collect*.
[26] *See generally* Lyft Privacy Policy.
[27] Uber Privacy Policy, *Information We Collect* and *How We Use Your Information*.
[28] Sidecar Privacy Policy 1(4), (6).

the third parties' privacy policies.[29] While Uber allows users to opt out of tracking for advertising purposes,[30] Sidecar's privacy policy states that users may opt out only by disabling cookies on their browser and location and UUID-sharing on their devices – making opt-out a non-option because doing so would disable the application's features.[31]

C. Location and Usage History Information

Although Uber, Sidecar and Lyft each offer somewhat different features, their mobile-based functionality operates similarly: a customer hails a driver, tracks a driver's arrival time and pays for the transportation all through an application on his or her mobile device.[32] The mobile applications collect GPS location data from the driver and customer's respective mobile devices to match customers to nearby drivers, establish pick-up and drop-off locations and calculate fares.[33] In the case of Lyft and Sidecar, the customer also uses the mobile device to pay the driver at the end of the trip.[34] Over the course of one transaction, an application therefore collects information (at least) about customer's identity and the origin, destination, trajectory, date, time and cost of his or her trip. Apart from ride-related information, Sidecar also collects messages sent between users through the application.[35]

## III. POTENTIAL PRIVACY ISSUES

Consumer privacy issues include substantive issues regarding what companies actually do with the customer information that they collect and procedural issues regarding notice of company practices and user choice or control over information about them. Here, EFF merely highlights a few issues that appear on the surface of the ridesharing services' privacy policies.

---

[29] *Id.* at 2(b).
[30] Uber Privacy Policy, *Targeted or Behavioral Advertising*.
[31] Sidecar Privacy Policy 4(b).
[32] *See* Uber, *Learn More*, http://www.uber.com/cities (last visited Feb. 7, 2013); Lyft, *Get Ready for Lyft Off!* (Aug. 23, 2012), http://blog.lyft.me; Sidecar, *FAQ*, http://www.side.cr/faq (last visited Feb. 7, 2013).
[33] *Id.*
[34] *See* Sidecar, *FAQ*; Lyft, *Help*, http://help.lyft.me (last visited Feb. 7, 2013).

As noted above, law enforcement access to customer information raises significant privacy concerns. All three services warn that they may disclose individual customer information if required to do so by law or subpoena, to cooperate with law enforcement, and in other situations at the services' discretion. Sidecar's privacy policy states that it may disclose information where it "reasonably believe[s] such action is necessary" to comply with "reasonable requests of law enforcement," to enforce Sidecar's terms of service, or to secure the rights and safety of the company and its users.[36] Uber reserves the right to disclose user information at its "sole discretion" in the same circumstances as Sidecar and also "to prevent or stop activity [Uber] may consider to be, or to pose a risk of being, an illegal, unethical or legally actionable activity,"[37] while Lyft states it will do so where required by law, to cooperate with police, or for safety reasons.[38]

In explaining its information collection practices, however, Uber's privacy policy also states that: "We will not share this information with third parties for any purpose and will only use this information for the sole purpose of fulfilling your request."[39] This statement seems to cover most, if not all, of the information that Uber itself collects, including geolocation information—in apparent conflict with its law enforcement access policy.

The privacy impacts of such disclosure policies depend to some extent on how long the companies keep user information. Data minimization – not keeping user data longer than is

---

[35] Sidecar Privacy Policy 1.
[36] Sidecar Privacy Policy 2(a)(iv).
[37] Uber Privacy Policy, *Our Disclosure of Your Information* ("the Company cooperates with government and law enforcement officials and private parties to enforce and comply with the law. We will disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to respond to claims and legal process (including but not limited to subpoenas), to protect the property and rights of the Company or a third party, to protect the safety of the public or any person, or to prevent or stop activity we may consider to be, or to pose a risk of being, an illegal, unethical or legally actionable activity.").
[38] Lyft Privacy Policy, *Special Cases in Which We Share Personal Information* ("We may also disclose personal information when We determine that such disclosure is necessary to comply with applicable law, to cooperate with

necessary – is a basic privacy principle. Stored user data can attract law enforcement as well as civil litigants interested in a user's locations or activities. Data retention also implicates data security concerns. While all three companies state that they employ commercially reasonable measures to secure the data, such as firewalls and encryption, all three acknowledge the risk of a potential security breach.[40] Further, Sidecar and Lyft's policies both warn that user data may be transferred and stored in other countries whose laws offer weaker protection for privacy than U.S. law.[41]

The companies' privacy policies unclearly suggest that they indefinitely retain much, if not all, of the information they collect from users. Uber provides the most detail, stating that it maintains personal user information – including trip history information and geolocation data – "as long as [an] account is active or as needed to provide [the user] services."[42] Its privacy policy states that Uber retains the information "to closely monitor which features of the Service are used most, to allow [users] to view [their] trip history, store [user] credit card information on a secure page, view any promotions [Uber] may currently be running, rate trips, and to determine which features [Uber] need[s] to focus on improving."[43] Lyft and Sidecar's privacy policies specify what types of data they collect, but they do not specify whether they also retain specific types of data or for how long.[44]

Although all three companies allow users to amend their personal information, only Uber and Lyft give users some choice on what happens to their data after terminating the account, and all three services retain user data for some period of time beyond the lifetime of the account. An

---

law enforcement or to protect the interests or safety of Lyft or other visitors to the Lyft Platform.").
[39] Uber Privacy Policy, *How We Use Your Information*.
[40] Sidecar Privacy Policy.at 3(b)-(c); Lyft Privacy Policy, *Our Security Precautions*; Uber Privacy Policy, *Security*.
[41] Sidecar Privacy Policy 3(a); Lyft Privacy Policy, *Our Security Precautions*.
[42] Uber Privacy Policy, *Access to Personal Information*.
[43] *Id.*, *How We Use Your Information*.
[44] Sidecar's policy specifies only that it retains "profile information" and "User Content" beyond the lifetime of the

Uber user can request by email to amend or correct their personal information or, by terminating their account, "request that [Uber] no longer use [the] information to provide [the user] services."[45] Nevertheless, Uber's policy states that it "will retain and use [the user's] information as necessary to comply with [Uber's] legal obligations, resolve disputes, and enforce [its] agreements."[46] Although Lyft's privacy policy promises to give "Users the option to remove their information from [its] database,"[47] elsewhere the policy states that "standard procedure" is to retain user-submitted information for an "indeterminate length of time."[48] Sidecar offers users no say in the disposal of their personal information, stating that after an account is closed, the company will retain user data "for a commercially reasonable time for backup, archival, or audit purposes."[49]

Also important here is adequate notice to users. None of the policies that we looked at provides for informing customers, before or after disclosure, about requests for their information from law enforcement or other parties. More generally, each of the three privacy policies contains some provisions that may not adequately inform consumers about how a provider will handle their private information. For example, although Lyft's policy acknowledges that it works with third-party advertisers, it does not, unlike its two other competitors, specify under what terms those third parties may collect user information through Lyft's website or mobile application.[50] And only Uber promises to inform users by email of changes to its privacy policy.[51] Lyft's policy states that the company will inform users of changes, but elsewhere states that it may also change a policy without notice if the new policy applies only to prospective data

---

account. Sidecar Privacy Policy 4(c).
[45] Uber Privacy Policy, *Access to Personal Information*. The extent to which such requests are honored is unclear.
[46] *Id.*
[47] Lyft Privacy Policy, *Choice/Opt-Out*.
[48] *Id.*, *Information Retention*.
[49] Sidecar Privacy Policy 4(c).
[50] *See generally* Lyft Privacy Policy.

collection and use.[52] Sidecar states that it may change its privacy policies "from time to time" and encourages users to monitor the policy periodically for changes.[53] As mentioned earlier, a fourth mobile-based car service, InstaCab, offers only a five-sentence privacy policy that addresses only third-party advertising and data-storage security measures.[54]

Finally, user control over how their data is used varies considerably among the privacy policies. Uber customers can opt out only from use of their information for targeted advertising purposes.[55] They cannot, however, opt out from Uber's sharing their information with "trusted partners," and must contact each of those third parties directly to opt out from promotional communications from them.[56] Sidecar and Lyft let customers opt out only from receiving certain communications, but not from collection or use of their data.[57] Sidecar customers can opt out from data tracking only by changing the settings on their browsers and devices, which the company's policy acknowledges is impossible on some devices and in any event disables features required to use the service.[58]

## IV. CONCLUSION

The sensitivity of the data collected by mobile device-based transportation services makes clear the importance of ensuring that it is collected, stored and used with consumers' privacy and safety in mind. Taken as a whole, that data is capable not just of revealing who a user is and where he or she lives and works, but also of describing in minute detail his or her comings and goings.

---

[51] Uber Privacy Policy, *Changes to this Privacy Policy*.
[52] Lyft Privacy Policy, *Changing our Privacy Policy for Previously Gathered Information*.
[53] Sidecar Privacy Policy 8.
[54] InstantCab, *PRIVACY*, *supra* note 1.
[55] Uber Privacy Policy, *Targeted or Behavioral Advertising*.
[56] Uber Privacy Policy, *Our Disclosure of Your Information*.
[57] Sidecar Privacy Policy 4; Lyft Privacy Policy, *Choice/Opt-Out*.
[58] Sidecar Privacy Policy 4(b).

Accordingly, EFF believes that the Commission should address consumer information privacy and security issues in this proceeding.

Dated: February 11, 2013

Respectfully submitted,

By: /s/ Lee Tien

Lee Tien
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x 102
Facsimile: (415) 436-9993
E-Mail: tien@eff.org

Counsel for
ELECTRONIC FRONTIER FOUNDATION

**VERIFICATION**

I am the attorney for the Electronic Frontier Foundation and am authorized to make this verification on its behalf. I am informed and believe that the matters stated in this pleading are true.

I declare under penalty of perjury that the matters stated in this pleading are true and correct.

Executed on the 11th day of February, 2013, at San Francisco, California.

By: /s/ Lee Tien
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x 102
Facsimile: (415) 436-9993
E-Mail: tien@eff.org