BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

FILED
7-31-17
04:59 PM

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

REPLY COMMENTS OF CALIFORNIA MANUFACTURERS & TECHNOLOGY ASSOCIATION TO PHASE III.B MEMO & RULING OF ASSIGNED COMMISSIONER

TRACK 3 – TNC DATA

Jarrell Cook
California Manufacturers & Technology Association
1115 11th Street
Sacramento, CA 95814
916-498-4456
jcook@cmta.net

Dated: July 31, 2017 in Sacramento, California.

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

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

REPLY COMMENTS OF CALIFORNIA MANUFACTURERS & TECHNOLOGY ASSOCIATION TO PHASE III.B MEMO & RULING OF ASSIGNED COMMISSIONER

TRACK 3 – TNC DATA

In accordance with Rules of Practice and Procedure of the California Public Utilities Commission ("Commission"), the California Manufacturers & Technology Association ("CMTA") hereby submits these reply comments on Track 3 of the Commission's *Amended Phase III.B. Scoping Memo and Ruling of Assigned Commissioner* (R.12-12-011), relating to Transportation Network Company ("TNC") data.

I. INTRODUCTION

CMTA seeks to encourage policies that promote innovation, stimulate economic growth, and protect the business climate for California's 30,000 manufacturing- and technology-based companies. Our association represents the nation's leading manufacturing and technology companies in sectors ranging from defense to energy, infrastructure to automation. Specifically, CMTA represents major automobile companies and their suppliers – industries that are directly impacted by Track 3 of the Commission's *Amended Phase III.B. Scoping Memo and Ruling of Assigned Commissioner*. CMTA strongly encourages the Commission against the establishment of a website portal for TNC data, as well as against the release of TNC trip data with interested government entities beyond original regulatory intent.

In the opening comments submitted by the California Chamber of Commerce ("CalChamber"), Engine, the Internet Association ("IA"), Lyft, Inc., Raiser-CA, LLC ("Raiser") and the Technology Network ("TechNet"), parties emphasized the irreversible safety, privacy and cybersecurity risks of publicly releasing otherwise proprietary customer data. Participating parties also underscored the considerable capital and workforce investments each TNC has made in order to produce these market sensitive reports for the Commission. TNC user reports are currently filed annually under compulsion of law and under explicit assurances that privileged market data will be afforded strong protections. The Commission has long upheld the confidentiality of this competitively sensitive information. We urge the Commission to continue that practice.

Today's TNCs and ridesharing companies continue to develop innovative, affordable solutions to California's most pressing automotive and transportation issues, including, traffic congestion and rising GHG emissions negatively impacting air quality. TNCs also play an integral role in helping the State and affiliated governmental entities meet their transportation policy goals, such as VisionZero, by removing distracted or otherwise impaired drivers from the road. The release of proprietary and competitively sensitive data would unnecessarily impede TNCs' ability to help support these important environmental and safety goals. Accordingly, CMTA, along with the majority of the proceeding parties filing Track 3 comments, strongly cautions the Commission against publicizing TNC data absent any measurable public benefit and at the direct cost of individual customer and commercial privacy assurances.

II. OPEN TNC DATA WOULD STIFLE INDUSTRY INNOVATION AND ERODE MARKET COMPETITION.

The release of private consumer and company TNC data beyond the CPUC's original regulatory intent would impede innovation and erode market competition. Today, TNC companies are developing advanced transportation solutions to complement existing public transit systems. These solutions present affordable and reliable transportation options for consumers, while helping reduce congestion resulting from increased urban development, population growth, employment opportunities, road construction and limited parking. While U.S. traffic congestion accounted for over $300 billion in fuel and productivity costs in 2016,[1] a recent study by Lyft reported that over half of their users experienced reduced usage of their personal vehicles and nearly one-quarter of users use a ridesharing platform to connect to and from public transit.[2] This reduced dependence on personal vehicle ownership removes cars from the road, promotes public transit options and measurably impacts City congestion and air quality.

Further, the TNC industry is rapidly evolving, subject to an increasingly complex regulatory landscape. Companies are forced to make significant ongoing economic and workforce investments in order to comply with today's ever-changing TNC regulations. Relatedly, TNCs are forced to continually develop new product and service offerings to maintain their competitive edge in the market. Many of these business advantages are discoverable in the reports, which highlight information related to fare frequency, market demand by neighborhood, customers in a certain location or timeframe, ride routes, average trip distance, and how often fares are split or grouped. The public release of these reports would unnecessarily reveal trade secrets that otherwise allow TNCs to help meet market demand and promote the State's leading

[1] INRIX Study; Feb. 6, 2017; http://inrix.com/resources/inrix-2016-traffic-scorecard-us/
[2] Lyft 2017 Economic Impact Report

transportation goals. To date, no legitimate benefit has been presented that outweighs the substantial market and customer privacy risks that would result from TNC data disclosure. Publicizing TNC data filings would only allow market competitors and potential cyberhackers to identify sensitive TNC information, resulting in a groundless breach of proprietary business operations.

III. EVEN ANONYMIZED TNC DATA PRESENTS GRAVE CYBERSECURITY RISKS AT THE EXPENSE OF PASSENGER AND DRIVER SAFETY.

In opening comments provided by the Los Angeles Department of Transportation ("LADOT"), the San Francisco County Transportation Agency ("SFTCA"), San Francisco Airport, San Francisco Taxi Workers Alliance ("SFTWA") and the San Francisco City Attorney's Office ("City Attorney"), select parties suggested that the cybersecurity and privacy risks associated with the transmission of customer and market data would not occur if the data is afforded a certain degree of anonymity and relevant redactions. This is simply not true.

In reality, the maintenance of a public ridesharing database capable of adequately protecting driver and rider privacy requires a great degree of technical expertise and financial investments. Redactions of customer and driver information are an insufficient means of protecting highly-sensitive identifiable markers. Further, any additional access to TNC data beyond the Commission would only increase the vulnerability of a cyberattack. To that end, Track 3 parties cited a number real-world cybersecurity cases resulting from released anonymized data:

- In a 2014 case involving the New York City Taxi and Limousine Commission, publicly released anonymous and randomized trip information appearing innocuous to the

untrained eye was used to extract personal user data about drivers, including personal addresses and driver routes. [3]

- An MIT study titled, *Weaving Technology and Policy Together to Maintain Confidentiality*, found that anonymized medical data, when shared, can "be used to re-identify individuals by linking or matching the data to other databases…" [4]
- Researchers at the University of Texas at Austin used the anonymous movie ratings of 500,000 Netflix subscribers hosted on an open database to "demonstrate that an adversary who knows only a little bit about an individual subscriber can easily identify [a] subscriber's record in the dataset…uncovering their political preferences and other potentially sensitive information."[5]

CMTA maintains that there is no compelling benefit to publishing private TNC data without creating unnecessary and irreversible cybersecurity risks. Ultimately, local governments cannot 100% ensure that public data is not susceptible to security breaches, leaks or mismanagement.

IV. PUBLIC ACCESS TO TNC DATA VIOLATES CONSUMER TRUST WHILE UNNECESSARILY PUTTING CUSTOMERS AND DRIVERS AT RISK.

In opening comments submitted by CalChamber, Engine, IA, Lyft, and TechNet, parties reinforced the notion TNC data disclosure would be a violation of customers' reasonable privacy expectations. Importantly, it would do so without any direct benefit to consumers. As noted in Section III of our reply comments, cybersecurity and privacy breaches are real, irreversible risks and no existing government resources can 100% prevent a cyberattack. The information

[3] Alex Hern, "New York taxi details can be extracted from anonymized data, researchers say"; June 27, 2014; https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-dataresearchers-warn

[4] L. Sweeney. Weaving Technology and Policy Together to Maintain Confidentiality. *Journal of Law, Medicine & Ethics*, 25, nos. 2&3 (1997): 98-110.

[5] Narayanan, Arvind, and Vitaly Shmatikov. "Robust De-anonymization of Large Sparse Datasets." SP '08 Proceedings of the 2008 IEEE Symposium on Security and Privacy (2008): 111-25.

provided in reports – such as fare frequency, market demand by neighborhood, customers in a certain location or timeframe, routes, average trip distance, and how often fares are split or grouped – can be easily decoded to identify the personal information of customers and drivers. This can be done even if information is anonymized or redacted. Therefore, public access to TNC data would present significant privacy and security breaches at the direct harm of TNC customers and drivers.

V. NO LEGAL JUSTIFICATION EXISTS REQUIRING THE COMMISSION TO SHARE CUSTOMER PRIVACY AND COMPETITIVELY SENSITIVE MARKET DATA.

Sharing TNC trip data for public use lacks legal justification. According to opening comments submitted by the San Francisco City Attorney, the City Attorney's Office issued a June 2017 letter to the Commission requesting TNC data. The Commission denied this request, citing a prior PUC ruling that TNC data was afforded certain anti-disclosure protections. In opening comments, the City Attorney argues that the California Public Records Act (CPRA) mandates the release of the requested data. This is incorrect. CPRA does not require release of records when state law exempts a set of records from disclosure. =. Cal Gov Code § 6254(k). In this case, a state law, § 583 of the Public Utilities Code, exempts from disclosure records furnished to the commission by a utility, unless those records are "specifically required to be open to public inspection" by the Public Utilities Act or if the commission or a commissioner orders the records to be open to public inspection. The City Attorney has not cited a provision of the Public Utilities Act or an appropriate order indicating that TNC data is specifically required to be open to public inspection. In addition, CMTA notes , that the under the CPRA, data cannot reveal private data about passengers or drivers. As noted above in Section III of our reply

comments, even anonymized data can reveal private data about passengers or drivers.Therefore, the CPRA does not mandate TNC data disclosure, as it cannot be done without potentially compromising proprietary customer and driver information.

Additional proceeding parties cite established Commission practice and legal precedent that protect TNC data against public disclosure. Opening comments filed by Lyft and TechNet assert that TNC companies cannot be singled out for data disclosure while other industries under CPUC jurisdiction are provided this protection. For example, the Commission currently has access to private customer information provided by telecommunications companies, such as geo-locational information that could be used to identify and locate customers. Accordingly, the Commission has provided these records significant protections against public disclosure. No legitimate reasons exists to treat TNC customer information differently.

The Track 3 record already provides ample authority for the protection of TNC data, including:

- *California General Order 66-C §2,* establishing that "[r]eports, records and information requests or required by the Commission which, if revealed, would place the regulated company at an unfair business advantage are not public records and are not open to public inspection." Further, any data request must be directed to the Commission Secretary to determine if the requested records fall within the listed exclusions or "if there is some public interest served by withholding the records" (General Order 66-C §3.3).
- *Public Utilities Code §583,* establishing that "[n]o information furnished to the Commission by a public utility or any business which is a subsidiary or affiliate of a public utility, or a corporation which holds a controlling interest in a public

utility, except those matters specifically required to be open to public inspection by this part, shall be open to public inspection or made public except on order of the Commission, or by the Commission or a Commissioner in the course of a hearing or proceeding."

- *Public Utilities Code §5412.5*, establishing that it unlawful to share any information presented in the inspection of accounts, books, papers, or documents of a charter-party carrier of passengers, except as authorized by the Commission or a court.
- *Raiser, LLC v. City of Seattle (King County Sup. Ct. 2016)*, establishing pickup and drop-off zip code data as a valuable trade secret that would unfairly allow TNCs to influence strategic market and operational decisions if made public.
- *Los Angeles Unified School District v. Superior Court*, establishing that proprietary data provided by a regulated entity does not become disclosable simply because it has been submitted to an agency unless the data sheds light on the agency's actions.
- *Syngenta Crop Protection, Inc. v. Helliker*, establishing that trade secrets may not be made public unless a "serious injustice" would otherwise result. A trade secret is defined as any details that derive independent economic value that are not generally made public and from which an entity can obtain economic value from its disclosure.

As the above demonstrates, established Commission practices and procedures, as well as longstanding principles of California law, strongly favor retaining the privacy and security of TNC data. Accordingly, CMTA echoes the argument made by CalChamber, Engine, IA, Lyft,

and TechNet that no additional public benefit or sound legal precedent has been presented warranting the release of private TNC data.

VI. CONCLUSION

CMTA appreciates the opportunity to submit these reply comments on the Ruling and looks forward to working with the Commissioner on this matter.

Respectfully submitted,

/s/ Jarrell Cook

Jarrell Cook
California Manufacturers & Technology Association
1115 11th Street
Sacramento, CA 95814
916-498-4456
jcook@cmta.net

July 31, 2017