BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIF

FILED
06/21/22
04:59 PM
R1212011

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

MOTION OF LYFT, INC. FOR CONFIDENTIAL TREATMENT OF CERTAIN DATA IN ITS 2022 ANNUAL REPORT

Molly Zimney
Janeé C. Weaver
Regulatory Compliance Counsel
Lyft, Inc.
185 Berry St., Suite 5000
San Francisco, CA 94107
mollyzimney@lyft.com
(415) 475-8459

Daniel T. Rockey
Bryan Cave Leighton Paisner LLP
Three Embarcadero Center, 7th Floor
San Francisco, CA 94111
daniel.rockey@bryancave.com

(415) 268-1986
Attorneys for Lyft, Inc.

June 21, 2022

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)

MOTION OF LYFT, INC. FOR CONFIDENTIAL TREATMENT OF CERTAIN DATA IN ITS 2022 ANNUAL REPORT

Pursuant to Decision (D.) 20-03-014 ("D.20-03-014") and Rule of Practice and Procedure ("Rule") 11.4, Lyft, Inc. ("Lyft") seeks an order authorizing it to file under seal certain specifically identified portions of its 2022 Annual Report (due to be submitted on September 19, 2022) and providing that such portions shall be deemed confidential for purposes of Commission General Order 66-D ("GO 66-D").

I. INTRODUCTION

On December 21, 2020, the Commission issued an order on Lyft and Uber's 2020 motions for confidential treatment of their Annual Reports ("2020 Ruling"), ruling that certain fields could reveal the movements of individual users, implicate serious privacy concerns, and should be redacted from public versions of the reports.[1] The Commission affirmed the 2020 Ruling in Decision (D.) 22-05-003.[2] Although that decision is currently the subject of an Application for Rehearing ("Application"), and has been stayed at least until the Commission resolves the Application, no party has challenged the ALJ's 2020 Ruling to the extent it deems such fields confidential. Lyft relies upon that Ruling in seeking confidential treatment for those same categories of data in its 2022 Annual Report.

In addition to the categories of data deemed confidential by the 2020 Ruling, Lyft seeks confidential treatment of those categories that were the subject of its appeal of the ALJ's 2020 Ruling and its Application, which Lyft's refers to as Trip Data, as well as three new categories of Trip Data added by Consumer Protection and Enforcement Division staff for 2022.[3] In Seeking

[1] Assigned Administrative Law Judge's Ruling on Uber Technologies, Inc.'s and Lyft's Motion for Confidential Treatment of Certain Information in their 2020 Annual Reports ("2020 Ruling").
[2] Decision Denying Appeal Of Lyft, Inc. Re: Ruling Denying, In Part, Motions By Uber Technologies, Inc. And Lyft Inc. For Confidential Treatment Of Certain Information In Their 2020 Annual Reports (D.22-05-003), p. 124.
[3] Lyft refers to all of the data, including the new categories, as Trip Data.

confidential treatment for categories for which confidential treatment was denied in D.22-05-003, Lyft notes that the 2020 Ruling – which that decision affirmed – held only that the evidence submitted in support of the 2020 motions for confidential treatment was insufficient to carry the TNCs' burden. It did not rule that a need for confidentiality could not be shown on a more fulsome evidentiary record. Furthermore, as Lyft has yet to exhaust its administrative remedies, and is entitled to seek judicial review of D.22-05-003 in the event rehearing is not granted, Lyft is entitled to – indeed is obligated to – seek confidential treatment for data which it considers to be a trade secret or the disclosure of which would represent an unwarranted invasion of the privacy rights of Lyft and its users.

II. BACKGROUND

A. Data Reports and Fields in 2021 Annual Reports

The templates provided by the Commission for the 2022 TNC Annual Reports include numerous individual reports, each with multiple data fields. The reports are labeled as follows:

- Driver Names & IDs
- Accessibility Report
- Accessibility Complaints
- Accident & Incidents
- Assaults & Harassments
- 50,000+ Miles
- Number of Hours
- Number of Miles
- Driver Training
- Law Enforcement Citations
- Off-platform Solicitation
- Aggregated Requests Accepted
- Requests Accepted
- Requests Accepted Periods
- Aggregated Requests Not Accepted
- Requests Not Accepted
- Suspended Drivers
- Total Violations & Incidents

- Zero Tolerance

Each of the foregoing reports includes various data fields, which are given an abbreviated descriptor by CPED staff, such as "DriverLicNum," "TripReqRequesterLat," "TripReqRequesterCB." In this motion, and the declaration which accompanies it, Lyft identifies each field for which confidential treatment is requested by first identifying the Report Name and then listing the abbreviated field descriptor provided by CPED.

B. Data Fields for Which Lyft Seeks Confidential Treatment

1. Data fields deemed confidential pursuant to December 21, 2020 decision on Lyft and Uber motions for confidential treatment

The ALJ's 2020 Ruling on Lyft's and Uber's motions for confidential treatment of the 2020 Annual Reports agreed with Lyft and Uber that certain fields in the TNC Annual Reports were confidential and should be redacted. Those fields include the following:[4]

Report	Field
Requests Accepted	
	Waybill1; Waybill2; Waybill3; Waybill4; Waybill5; Waybill6; Waybill7
	DriverID
	VIN
	AppOnOrPassengerDroppedOffLat; AppOnOrPassengerDroppedOffLong
	TripReqRequesterLat; TripReqRequesterLong
	TripReqDriverLat; TripReqDriverLong
	ReqAcceptedLat; ReqAcceptedLong
	PassengerPickupLat; PassengerPickupLong
	PassengerDropoffLat; PassengerDropoffLong
Requests Accepted Periods	
	DriverID
	VIN
	PeriodStartLat
	PeriodStartLong
	PeriodEndLat
	PeriodEndLong
Requests Not Accepted	

[4] The appendices to the ALJ's Confidentiality Ruling do not consistently track the descriptions given those fields by CPED. For clarity, Lyft has identified each specific field using the nomenclature provide by CPED in the 2021 templates.

	DriverID
	VIN
	TripReqRequesterLat
	TripReqRequesterLong
	TripRequesterDestinationLat
	TripRequesterDestinationLong
	NotAcceptedDriverLat
	NotAcceptedDriverLong
Assaults & Harassments	
	Waybill1; Waybill2; Waybill3; Waybill4; Waybill5; Waybill6; Waybill7
	DriverID
	VIN
	AssaultHarassLat
	AssaultHarassLong
	AssaultHarassType; AssaultHarassDef
	AssaultHarassDescr
Accidents & Incidents	
	Waybill1; Waybill2; Waybill3; Waybill4; Waybill5; Waybill6; Waybill7
	DriverID
	VIN
	IncidentAccidentLat
	IncidentAccidentLong
	AmountPaidAnyParty
	AmountPaidDriverIns
	AmountPaidTNC
	AmountPaidOther
Driver Names & IDs	
	DriverID
	DriverFirstName
	DriverMI
	DriverLastName
	DriverLicNum
	DriverLicState
	DriverLicExp
Accessibility Complaints	
	DriverID
50,000+ Miles	
	DriverID
	VIN
Number of Hours	
	DriverID
Number of Miles	
	DriverID

Law Enforcement Citations	
	Waybill1; Waybill2; Waybill3; Waybill4; Waybill5; Waybill6; Waybill7
	DriverID
	VIN
Off-platform Solicitation	
	DriverID
	VIN
	OffPlatformSolicitationLat
	OffPlatformSolicitationLong
Suspended Drivers	
	DriverID
Zero Tolerance	
	Waybill1; Waybill2; Waybill3; Waybill4; Waybill5; Waybill6; Waybill7
	DriverID
	VIN
	ZeroToleranceLat
	ZeroToleranceLong

No party has challenged the 2020 Ruling on the confidentiality of these fields, which remain essentially unchanged from the 2020 Annual Report templates. The Commission reversed the 2020 Ruling with respect to the Waybills category, which was expanded in 2021 to include multiple Waybill cells and which carries through to the 2022 Annual Reports.[5] Lyft does not challenge that reversal and therefore does not seek confidential treatment for Waybill numbers. Lyft otherwise relies upon the ALJ's 2020 Ruling, and the evidence and argument submitted in its 2020 motion for confidential treatment, in seeking confidential treatment for the same data in the 2022 Annual Reports.[6]

2. Lyft seeks confidential treatment of the following additional fields in the 2022 Annual Report

[5] The Confidentiality Ruling approved redaction of Waybill ID. For the 2021 Annual Report, CPED created multiple Waybill fields (e.g., Waybill 1, Waybill 2, Waybill 3, etc.), which have carried over to the 2022 Annual Reports. However, in the Administrative Law Judge's ruling on the 2021 Annual Reports [Ruling Granting, In Part, The Motions Of Uber Technologies, Inc., Lyft, Inc., Hopskipdrive, Inc., And Nomad Transit, LLC For Confidential Treatment Of Portions Of Their 2021 Annual Transportation Network Company Reports ("2021 ALJ Ruling")], the Commission reversed this decision concerning the confidentiality of Waybill data, finding that they should not be redacted. 2021 ALJ Ruling, p. 5-6.

[6] Motion of Lyft, Inc. for Confidential Treatment of Certain Information in Its 2020 Annual Report ("2020 Lyft Motion").

The 2020 Ruling "agree[d] with Moving Parties with respect to the latitude and longitude of both the driver and rider of a particular TNC trip," finding "[s]upport for the proposition that this information might be engineered to identify the exact starting and ending addresses of a trip, which can then be combined with other information to identify a driver and/or passenger."[7] However, the 2020 Ruling "disagree[d] with Moving Parties' request that the balance of the geolocational data (date and time, census block and zip code of both the driver and rider; when the rider is picked up and dropped off; when the driver's app is turned on or the last rider dropped off; time a trip request was made; and when the trip request was accepted on the TNC's app) should be treated as confidential and redacted from the public version of the 2020 Annual Reports."[8] The Ruling found that "Moving Parties have failed to make the necessary granular showing how this geolocational data, either individually or in combination, could lead to the identification of a particular driver or customer."[9]

Lyft appealed to the Commission, seeking review of the portion of the 2020 Ruling that denied confidential treatment for "the balance of the geolocational data" relating to specific TNC trips. The Commission has since issued D.22-05-003, denying Lyft's Appeal as to the 2020 Annual Reports. However, Lyft has sought rehearing of that decision and the Commission subsequently granted Lyft's motion for a stay of the decision at least until the Application for Rehearing can be resolved.[10] Furthermore, the ALJ's 2020 Ruling and the ALJ's ruling on Lyft's 2021 motion for confidential treatment found only that Lyft had failed to submit sufficient evidence to support its claim. As a result, nothing precludes Lyft from seeking confidential treatment for data beyond that deemed confidential in the 2020 Ruling as to its 2022 Annual Reports. Based upon the ***new*** and ***additional*** evidence and argument submitted with this motion, Lyft seeks confidential treatment for the following additional fields in its 2022 Annual Report to be filed on September 19, 2022:

Report	Field
Requests Accepted	
	VehicleMake
	VehicleModel
	VehicleYear

[7] 2020 Confidentiality Ruling, p. 5.
[8] *Id.*
[9] *Id.*
[10] *See* Decision (D.) 22-06-023, Order Granting Stay Of Decision 22-05-003.

	AppOnOrPassengerDroppedOffZip
	AppOnOrPassengerDroppedOffTract
	AppOnOrPassengerDroppedOffCB
	AppOnOrPassengerDroppedOffDate
	TripReqRequesterZip
	TripReqRequesterTract
	TripReqRequesterCB
	TripReqDriverZip
	TripReqDriverTract
	TripReqDriverCB
	TripReqDate
	ReqAcceptedDate
	ReqAcceptedZip
	ReqAcceptedTract
	ReqAcceptedCB
	PassengerPickupDate
	PeriodTwoMilesTraveled
	PassengerPickupZip
	PassengerPickupTract
	PassengerPickupCB
	PassengerDropoffDate
	PassengerDropoffZip
	PassengerDropoffTract
	PassengerDropoffCB
	PeriodThreeMilesTraveled
	TotalAmountPaid
	PassengerPickupDatePrescheduled
	RideIDMilesTraveledP23
	RideIDMilesTraveledP3
Requests Accepted Periods	
	VehicleMake
	VehicleModel
	VehicleYear
	PeriodStartZip
	PeriodStartTract
	PeriodStartCB
	PeriodEndDate
	PeriodEndZip
	PeriodEndTract
	PeriodEndCB
	PeriodMilesTraveled
Requests Not Accepted	
	VehicleMake
	VehicleModel
	VehicleYear

	TripReqDate
	TripReqRequesterZip
	TripReqRequesterTract
	TripReqRequesterCB
	TripRequesterDestinationZip
	TripRequesterDestinationTract
	TripRequesterDestinationCB
	NotAcceptedDate
	NotAcceptedDriverZip
	NotAcceptedDriverTract
	NotAcceptedDriverCB
Assaults & Harassments	
	VehicleMake
	VehicleModel
	VehicleYear

Lyft notes that for the 2022 Annual Report, staff added a number of new fields. Of those newly added field, Lyft seeks confidential treatment for PassengerPickupDate, Prescheduled RideIDMilesTraveledP23, and RideIDMilesTraveledP3, as each of these fields, in combination with the remainder of the Trip Data, constitutes Trip Data which has independent value from not being generally known and could reveal the movements of Lyft users. For convenience, Lyft refers to all of this data collectively as "Trip Data." As explained below, Lyft seeks confidential treatment of the Trip Data on the grounds that the data constitutes a trade secret and may reveal private personal details of TNC users, and is therefore exempt from disclosure under the California Public Records Act.

III. LEGAL ANALYSIS

A. Private Companies Compelled to Submit Information to Regulatory Agencies Do Not Lose the Right to Protect their Data from Public Disclosure

1. That the Commission Requires Certain Data to Be Maintained Does Not Eliminate Lyft's Property and Privacy Interests in that Data

Before addressing the specific bases for confidential treatment of the Trip Data, it is important to consider several fundamental principles of law that impose limits on the ability of regulatory agencies to convert the private data of entities they regulate into a public good accessible to all. The first, and perhaps most fundamental, principle is that regulated entities do not lose the right to protect their data from public intrusion by virtue of being regulated. To the contrary, regulated entities retain both a possessory and ownership interest in the data generated in

the course of their business operations, and are entitled to all of the same rights and privileges as other citizens. As a result, administrative seizures of private company data must be narrowly tailored to serve a legitimate regulatory purpose of the agency which is informed by the regulatory scheme the agency seeks to enforce and must conform to other constitutional limitations, including the Fifth Amendment prohibition on unlawful "takings" (i.e., taking private property without just compensation). In the 2020 Ruling, and in D.22-05-003, the Commission appears to have consistently misunderstood Lyft's argument as to this issue. Lyft emphasizes these points not to contest the Commission's authority to require TNCs to submit Trip Data, but to demonstrate that prior to publicly disclosing data that Lyft is compelled to submit, the Commission must acknowledge Lyft's constitutional rights in that data and must lawfully justify its decision to destroy the secrecy of that data. It is the act of using the power of the State to force TNCs to publicly disclose Trip Data, which destroys its value and invades the privacy of Lyft and its users, that Lyft contests and which must be appropriately justified. In this regard, it is helpful to note that if the submission of data to a public agency destroyed any rights in that data, such that, once submitted, an agency can do as it pleases with the data, there would be no need for Government Code § 6254(c), 6354(k), or any of the other exceptions to the California Public Records Act; which are expressly concerned with avoiding the further invasion of rights that results from agency production of records in its possession.

In *Patel v. City of Los Angeles*, the Ninth Circuit addressed the authority of government agencies to demand access to the books and records of regulated entities.[11] In that decision, the court made clear that the "government may require businesses to maintain records and make them available for routine inspection when necessary to further a legitimate regulatory interest... [however,] the Fourth Amendment places limits on the government's authority in this regard."[12] Agency demands for access must be "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[13] Furthermore, the court explained, the fact that an entity is subject to government regulation does not thereby

[11] *Patel v. City of Los Angeles,* 738 F.3d 1058 (9th Cir. 2013), *aff'd sub nom. City of Los Angeles, Calif. v. Patel*, 135 S.Ct. 2443 (2015).
[12] *Patel*, 738 F.3d at 1064 (*citing California Bankers Ass'n v. Shultz*, 416 U.S. 21, 45–46, 94 S. Ct. 1494, 39 L. Ed. 2d 812 (1974)).
[13] *Id.*

transform its records into a public good.[14] This is because regulated entities retain "both a possessory and an ownership interest" in their books and records and have "the right to exclude others from prying into the contents of [those] records…."[15]

The Supreme Court affirmed the Ninth Circuit's decision, making clear that even as to pervasively regulated industries – which TNCs have never been determined to be – agency access to records must serve "a 'substantial' government interest that informs the regulatory scheme pursuant to which the inspection is made" and "the warrantless inspections must be 'necessary' to further [the] regulatory scheme."[16] Importantly, the fact that a regulated entity is required by law to maintain certain records does not eliminate the entity's right of privacy in those records. As the Supreme Court explained, regulated entities "retain[] that expectation of privacy notwithstanding the fact that the records are required to be kept by law."[17]

In the time since the Supreme Court issued its decision in *Patel*, other courts have applied that holding to nonpublic user data generated by online platforms similar to TNCs, including the peer-to-peer rental platform Airbnb. In *Airbnb, Inc. v. City of New York*, the City enacted an ordinance requiring short-term rental platforms to provide monthly disclosures of rental data to the city. The District Court held that such administrative demands for data of private companies likely violated the companies' 4th Amendment rights, explaining:

> [A]s the Ninth Circuit observed in *Patel*, customer-facing businesses, including in hospitality industries, "do not ordinarily disclose, and are not expected to disclose ... commercially sensitive information" such as "customer lists," other customer-specific data, and "pricing practices." [citation] ("The businessman, like the occupant of a residence, has a constitutional right to go about his business free from unreasonable official entries upon his private commercial property."); [citation] As in *Patel*, where the hotels were held to have a Fourth Amendment interest in the records of their guests, this Court holds that platforms have privacy interests in their

[14] 738 F.3d at 1061–1062.

[15] *Id.* at 1061.

[16] *Patel*, 135 S.Ct. at 2456.

[17] *Id.* at 1062; *McLaughlin v. Kings Island, Div. of Taft Broad. Co.,* 849 F.2d 990, 995–96 (6th Cir.1988) (even in a pervasively regulated industry, that company is required to maintain records does not eliminate "recognizable privacy interest" in those records nor make them "public property."); *Brock v. Emerson Elec. Co.,* 834 F.2d 994, 996 (11th Cir.1987) (fact that records are required by law to be kept "does not serve to strip away a company's attendant privacy interest in that information.").

> user-related records that "are more than sufficient to trigger Fourth Amendment protection."[18]

As the court further explained:

> Like a hotel, a home-sharing platform has at least two very good reasons to keep host and guest information private, whether as to these users' identities, contact information, usage patterns, and payment practices. One is competitive: Keeping such data confidential keeps such information from rivals (whether competing platforms or hotels) who might exploit it. The other involves customer relations: Keeping such data private assuredly promotes better relations with, and retention of, a platform's users.[19]

The court thus concluded that the city's interest in regulating short-term rentals did not "deprive the platforms of the right to claim a reasonable expectation of privacy in their business records chronicling their dealings with customers."[20]

Similarly, in *Airbnb, Inc. v. City of Boston,* the court held that "Airbnb has a reasonable expectation of privacy in the nonpublic usage data for its listings—especially when paired with additional information such as the location of the unit—and that the City cannot lawfully require disclosure of that information without the protections guaranteed by the Fourth Amendment (protections which are not accounted for in the Ordinance)."[21] The very same principles apply to the data collected by Lyft's and Uber's online platforms.

First, and perhaps most importantly, the above decisions make clear that although TNCs may be subjected to warrantless administrative demands for data, such as the Annual Report requirement here, the requirement to submit data to the Commission does not deprive TNCs of their constitutionally protected privacy and property interests in that data. As this point has been consistently misunderstood, Lyft repeats it here for emphasis. Lyft does not contest the Commission's authority to require submission of the Trip Data in the first instance. Lyft cites these decisions to make clear that, notwithstanding the Commission's requirement to submit Trip Data, Lyft nevertheless retains a constitutionally protected property and privacy right in its data. Those rights do not evaporate upon submission to the Commission. If they did, there would be no need

---

[18] *Airbnb, Inc. v. City of New York*, 373 F. Supp. 3d 467, 484(S.D.N.Y. 2019), *appeal withdrawn*, No. 19-288, 2019 WL 3492425 (2d Cir. May 9, 2019)

[19] *Id.* at 484.

[20] *Id.*

[21] *Airbnb, Inc. v. City of Boston*, (D. Mass. 2019) 386 F.Supp.3d 113, 125, appeal dismissed (1st Cir., Sept. 3, 2019, No. 19-1561) 2019 WL 6522166

for the various exceptions to the California Public Records Act, particularly including § 6254(c), which expressly recognizes the existence of privacy rights in records maintained by government agencies. As a result, any decision to order disclosure of Lyft's Trip Data must address Lyft's own property and privacy rights in that data, and must justify the decision to destroy them over Lyft's objections in accordance with applicable law.

Second, although the foregoing decisions recognize the Commission's authority as a government agency to compel TNCs to submit data, the exercise of that power must serve the Commission's own, narrowly tailored regulatory purpose, informed by the relevant statutory scheme. It is not authorized to collect data the Commission itself does not use for the purpose of turning it over to local agencies, or others, for their own purposes. Thus, any decision to require disclosure of TNC Trip Data cannot be justified not by the Commission's regulatory power. It may be ordered solely pursuant to the CPRA and consistent with the exceptions and limitations therein. If local agencies believe that TNC data is necessary, or would be useful, for their own regulatory purposes, their remedy is to petition the California legislature for authority to demand access to such data. The Commission may not employ its regulatory authority to seize the data from TNCs and then publicly expose it in the interest of providing access to local agencies for their own purposes.

B. The Trip Data Constitutes a Trade Secret and Cannot Be Disclosed in the Absence of Fraud or Injustice

Under the California Uniform Trade Secrets Act ("CUTSA"), a trade secret is "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[22]

In support of this Motion, Lyft has submitted the sworn declaration of Lyft's Vice President of Compliance, Alix Rosenthal, which attests, under penalty of perjury, to the following facts, which plainly establish both elements of §3426.1 with respect to the Trip Data. As Rosenthal explains:

[22] Civ. Code §3426.1(d); see also D.20-12-021, at *17.

> The Trip Data includes an array of information regarding ***every*** ride request on the Lyft platform during the reporting period. The Trip Data is among the most sensitive and valuable data collected and maintained by Lyft. Trip data is captured using data collection, analysis and reporting processes developed by Lyft over time and at great effort and expense. These processes continually capture events occurring across the Lyft platform and store the resulting data in Lyft's proprietary databases. The data is used in Lyft's operations and is compiled for both regulatory reporting ***and*** business analytics purposes. In addition to enabling Lyft to adapt to continually-evolving regulatory requirements, the data provides Lyft with critical insights into the effectiveness of its services, features, and marketing and promotional efforts, and helps Lyft to create an exceptional user experience for passengers and drivers.[23]

She continued:

> 11. Importantly, although Lyft formats the Trip Data (and other trip data which includes precise latitude and longitude and other details) to conform to CPED data reporting requirements when submitting its Annual Reports, that very same data has substantial value wholly apart from its value in allowing Lyft to comply with regulatory requirements. The data is continually collected, compiled, and analyzed as an integral aspect of Lyft's business operations, as the success of Lyft's business model depends upon continually optimizing the balance between ride demand and vehicle supply. Lyft endeavors to optimize supply and demand by using competitive pricing and promotions, such as ride credits and other discounts, to stimulate passenger demand, while increasing the supply of vehicles to areas with high demand by offering drivers minimum hour guarantees, bonuses, and other driver incentives. Lyft is continually adjusting these two levers to ensure, on the one hand, that fares and/or discounts are sufficiently enticing to attract passengers, and, on the other hand, that fares and driver promotions and incentives are sufficiently enticing to attract enough drivers to meet demand at any given time. This delicate balance is central to Lyft's competitiveness in California and in markets nationwide and the Trip Data allows Lyft to dynamically evaluate the effectiveness of its promotional, advertising, and incentive campaigns used to balance supply and demand. For example, by comparing the number and variety of rides completed during a particular time period in a particular area (e.g., a zip code, census block, city, or county) against the driver incentive programs deployed during that period for that area, Lyft can gauge the effectiveness of those incentives in

[23] Declaration of Alix Rosenthal in Support of Request Of Lyft, Inc. for Confidential Treatment of Certain Data In Its 2022 Annual Report ("Rosenthal Decl."), at ¶10.

> increasing the supply of drivers and can adjust its incentive programs going forward. Similarly, by cross-referencing the number and variety of rides against the particular passenger promotions run at that time, Lyft can track, assess, and understand the efficacy of its passenger-directed promotions, and can adjust them accordingly. Equally important, Lyft can identify those promotions that are ineffective and can avoid further expenditures on ineffective promotions. The ability to effectively measure the real-world effectiveness of its promotions and incentives using metrics collected during each individual trip allows Lyft to save a tremendous amount of time and effort on ineffective campaigns or promotions. To the best of my knowledge, no other company or individual has the ability to collect the same data from rides completed on the Lyft platform, making Lyft's Trip Data unique and distinct from data sets that may be collected by other TNCs concerning rides on their platforms, or by other companies from vehicle-connected GPS systems or processes. There is no other source of this extremely valuable data and to Lyft's knowledge, no one else maintains or is capable of generating the same compilation of data elements as those contained in Lyft's Trip Data..[24]

Rosenthal further explains that the Trip Data would be extremely valuable to Lyft's competitors for similar reasons:

> If Lyft's competitors, including Uber, HopSkipDrive, Wings, Silver Ride, Nomad Transit, and any other company that has obtained or might wish to obtain a TNC permit from the Commission, were provided access to Lyft's Trip Data, they could and would analyze and manipulate that data to gain insights into Lyft's market share, its pricing practices, its marketing strategies, its route optimization algorithms, and other critical aspects of its business that it does not publicly disclose. For example, the Trip Data would allow competitors to identify neighborhoods or portions of neighborhoods (defined by census block or zip code) in which Lyft drivers complete the greatest numbers of rides, allowing them to target these passenger rich areas. Alternatively, such competitors could identify areas of low activity, allowing them to profitably avoid such areas. Without access to Lyft's data, it would be extremely difficult and costly to obtain the same insight into these important commercial realities. Furthermore, because Lyft's fares and promotions are, by their nature, publicly accessible, if competitors had access to the Trip Data they could track those fares and promotions and analyze how the number or variety of rides fluctuated in response to changes in fares or promotional activities. They could then adjust their fares, or copy those promotions that the data shows were successful, in order

[24] Id. at ¶11.

> to drive new customers to their platforms. Such insights would be enormously valuable to a competitor, who would not need to invest the significant resources that Lyft has invested to test these programs and analyze the data to understand the market and optimize revenue generation. A new competitor could enter the market with a substantially reduced investment in money and human resources, while existing competitors could use the data to increase their market share, reduce their costs, or undercut Lyft's marketing campaigns, by "free-riding" on Lyft's data. I am confident in these assessments as I know that if Lyft were to obtain access to the trip data of its competitors, Lyft would analyze the data to assess the competitor's market share, its promotional initiatives, and other aspects of its business operations to gain insights that might be useful to Lyft in modifying its promotions or operations.[25]

Equally important, Rosenthal also explains that GPS-derived mobility data, like the Trip Data at issue here, has tremendous value to a wide variety of businesses for a variety of purposes – not only Lyft's competitors – and that Lyft has, in fact, been contacted by at least one third party who expressed interest in purchasing access to anonymized trip data:

> 1. It is my opinion, based upon my years of experience in the TNC field and prior work with vehicle data analytics, that mobility data collected from GPS-connected vehicles or mobile devices in vehicles, such as the Trip Data here, has enormous commercial value for a variety of purposes and organizations, not just TNCs. In fact, I am aware that an active market has developed for the sale or licensing of such data. For example, a company called Datarade hosts an online marketplace to facilitate the sale or licensing of GPS mobility data. The website and online marketplace can be found here: https://datarade.ai/data-categories/mobility-data. I am also aware of another company called Streetlight Data, which is focused on selling "anonymized location records from smart phones and navigation devices in connected cars and trucks." The website for Streetlight Data can be found here. https://www.streetlightdata.com/our-data/. In addition, I am aware that consulting firms, such as McKinsey & Co, have issued reports analyzing the monetary value of mobility data collected from smart phones and GPS connected vehicles – essentially the same data at issue here. See "Unlocking the Full Life-Cycle Value from Connected Car Data," at https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data#; see also "Car Data: Paving the Way to Value-Creating Mobility," at https://www.the-digital-insurer.com/wp-content/uploads/2016/05/704-mckinsey_car_data_march_2016.pdf. McKinsey & Co, is a well-known and highly regarded consulting firm. Each of the foregoing authorities helps to confirm my own view that vehicle–connected mobility data, such as Lyft's

[25] Id. at ¶12.

> Trip Data, has tremendous economic value for a variety of purposes wholly apart from Lyft's use of the data for its own operations or for compliance purposes. In fact, I am aware that at least one non-TNC entity has inquired of Lyft regarding the purchase or licensing of Lyft's Trip Data. The fact that third parties would be willing to pay Lyft for the right to access or license its Trip Data is alone sufficient to satisfy the second requirement of Civil Code §3426.1(d), that it is information that derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use.[26]

Finally, Rosenthal establishes that Lyft takes commercially reasonable measures to maintain the secrecy of the Trip Data:

> 1. Lyft stores the Trip Data on a secure software network protected by appropriate computer security controls, access to which is limited to a subset of Lyft employees who have been individually approved and use such information only to fulfill their job functions. Lyft also requires, as a condition of employment, that all new employees sign a confidentiality agreement. This agreement is put in place to protect Lyft's proprietary information from being disclosed by employees or former employees to unauthorized outside parties. The company also requires all employees to sign Lyft's employee handbook, which describes in detail each employee's obligations regarding technology use and security and protection of Lyft's confidential and proprietary information; and requires all visitors to Lyft headquarters to read and sign a non-disclosure agreement before proceeding past the reception desk. Furthermore, since the Commission issued General Order 66-D, Lyft has consistently complied with that order in seeking confidential treatment for the data it has identified as confidential herein, and otherwise vigorously protects such information from public disclosure. Significantly, although an individual driver or passenger would be aware of the location where a given ride commenced and terminated, individual drivers and passengers are not given access to rides completed by other drivers or passengers, or to the larger compilation of millions of rides completed over the course of a year that is included in the Annual Report.[27]

The foregoing evidence presented by Lyft plainly establishes that the Trip Data constitutes a trade secret under Civ. Code § 3426.1(d); *i.e.*, that the data has independent value from not being known to those who might make use of it and that it is the subject of reasonable efforts to maintain its secrecy. As the Commission itself recently recognized:

> [I]f a company 1) has invested resources to obtain information it can choose to withhold or make known to others, 2) can identify such information in a manner sufficient to distinguish it from matters of general knowledge, 3) has made reasonable efforts to protect

[26] Id., at ¶13.
[27] Id., at ¶14.

> the secrecy of the information (e.g., marking information as a trade secret, educating employees regarding such status, imposing strict controls, limiting physical or electronic internal and external access to the information, requiring nondisclosure agreements), 4) and can demonstrate that the secret information has independent economic value by virtue of being secret (as evidenced, for example, by the willingness of others to pay for the secret information), the company may have a protectable trade secret.[28]

Lyft has invested substantial resources in the systems and processes that allow it to collect the Trip Data, has specifically identified the components that make up that data, takes reasonable efforts to maintain the secrecy of that data, and has demonstrated that it has independent economic value, including by showing that others would be willing to pay for it. Thus, the Trip Data is protected from disclosure pursuant to Government Code §6254(k) and Evidence Code §1060 and may only be disclosed if the Commission correctly determines that redaction of such data would conceal fraud or work an injustice. There is no evidence that the failure to disclose such data would conceal a fraud or work an injustice.

1. D.22-05-003 Erroneously Applies a Uniqueness or Novelty Requirement for Demonstrating Trade Secret That Does Not Exist Under Applicable Law

In D.22-05-003, the Commission held that Lyft's Trip Data did not constitute a trade secret because Lyft failed to meet a purported novelty or uniqueness requirement. This was clear error, as California does not recognize a novelty or uniqueness requirement for trade secrets. As explained above, Civil Code § 3426.1 sets forth two requirements to establish a trade secret. The proponent must show that it is information which:

> (1) Derives independent economic value, actual or potential, from not being generally known to the public or other persons who can obtain economic value from its disclosure or use; and
>
> (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

D.22-05-003 acknowledged this provision, but nevertheless went on to hold that Trip Data is not trade secret because Lyft failed to prove the data is "novel or unique."[29] D.22-05-003 cites *Morlife v. Perry* (1997) 56 Cal. App. 4th 1514, 1523 as support for a "uniqueness requirement," but *Morlife* does not require a proponent of a trade secret to show that the secret is novel or unique. Instead,

[28] Decision Addressing Carriers' Confidentiality Claims Related To Network Study Ordered In Decision 13-02-023, As Affirmed In Decision 15-08-041, Decision 20-12-021, 2020 WL 7862639 (Cal.P.U.C.), at *14.
[29] D.22-05-003, p. 32.

the court in *Morlife* found that a customer list composed of publicly available contact information was a trade secret and that plaintiff need only show the compilation of elements is "not generally known to the public" to "satisf[y] … the first prong of the statutory definition of a 'trade secret.'"[30] D.22-05-003 argues that because the court noted the specialized nature of Morlife's roofing business in rejecting an argument that its customer list was not protectable, *Morlife* supports a uniqueness requirement, but in so doing, mistakes the requirement that a trade secret be secret (i.e., not generally known) for a requirement that it be unique. *Morlife* noted the specialized nature of Morlife's customer list in rejecting an argument that "there is nothing inherently secret or confidential about Morlife's customer base as all commercial buildings will need either repairs to an existing roof or a new roof." 56 Cal. App. 4th at 1523. In other words, the customer list would have no value if it was already generally known that every potential customer would need a new roof. Nothing about that holding requires a trade secret claimant to establish that its trade secret is novel or unique; only that it is not generally known to those who would make use of it.

D.22-05-003 also cites *US v. Nosal* (9th Cir. 2016) 844 F.3d 1024, but *Nosal* also does not support a uniqueness requirement. The Decision cites the following passage as evidence of a uniqueness requirement:

> Nosal takes the view that the source lists are merely customer lists that cannot be protected as trade secrets. This characterization attempts to sidestep the unique nature of the source lists, which are the customized product of a massive database, not a list of well-known customers.[31]

Again, this quote pertains to the ***secrecy*** element, not an unstated but implied "uniqueness" element. *Nosal* notes the "unique nature" of the source lists to distinguish them from lists that are "well-known" and thus not secret. Nowhere does it purport to create a new and distinct requirement beyond those imposed by the Legislature in § 3426.1 – nor could it. A court is not any more entitled to add to or amend the definition adopted by the Legislature than is the Commission, as neither is part of the legislative branch or otherwise empowered to make such policy judgments.

D.22-05-003 strains to find support for a uniqueness requirement by also citing *Conseco Finance Servicing Corp. v. North American Mortgage Co.* (8th Cir. 2004) 381 F.3d 811, a decision applying Missouri law. The court in that case found that although the lead sheets at issue contained

[30] 56 Cal. App. at 1523.
[31] 844 F. 3d, at 1043.

public information, they were not generally known because the computer program that generated them – which, notably, was ***not*** the claimed trade secret – "was uniquely Conseco's." 381 F. 3d, at 819. That is, the court held that the sheets were not generally known, even though they contained public information, because they had been generated by a unique software program. It did not impose a uniqueness requirement, contrary to the suggestion in D.22-05-003.

D.22-05-003 also curiously relies upon two decisions applying Washington law,[32] but those decisions, like D.22-05-003, mistake the "not generally known" requirement for a need to show information is unique to be trade secret. Not only do these decisions not apply here, they are bad law and it is a mistake for the Commission to have relied upon them. Further, the reliance upon these Washington decisions to justify a uniqueness requirement is particularly problematic here because D.22-05-003 declines to follow the holding of the Washington Supreme Court in *Lyft, Inc., et al., v. City of Seattle* (2018) 190 Wn.2d 769, in which the Washington Supreme Court found that even less granular trip data than that at issue here constitutes a trade secret under Washington law. It is all the more puzzling that D.22-05-003 attempted to distinguish *City of Seattle* on the grounds that "there was no discussion or finding that the compilation was novel or unique, which is a requirement under California law."[33] That is, D.22-05-003 relies upon Washington law as support for a uniqueness requirement in California that does not exist and then rejects the Washington Supreme Court's ruling on the very issue before this Commission on the grounds that Washington has no uniqueness requirement. These utterly contradictory rulings cannot be reconciled. The Commission should correct this error here.

Contrary to D.22-05-003, there is no novelty or uniqueness requirement for trade secret protection. Put simply, "[n]ovelty, in the patent law sense, is not required for a trade secret." *Kewanee Oil Co. v. Bicron Corp.* (1974) 416 U.S. 470, 476; *BladeRoom Group Ltd v. Emerson Elec. Co*. (N.D. Cal. 2018) 331 F.Supp.3d 977, 981, *vacated and remanded* (9th Cir. 2021) 11 F.4th 1010, *and vacated and remanded* (9th Cir. 2021) 20 F.4th 1231 ("Information need not be complex, novel or outside the understanding of a layperson to constitute a trade secret."); *Graduation Solutions LLC v. Luya Ent. Inc.* (C.D. Cal., May 5, 2020, No. CV191382DMGJPRX)

[32] D.22-05-003, p. 37. The two Washington decisions cited by the Decision cite to *Machen, Inc. v. Aircraft Design, Inc*. (Wash. Ct. App. 1992) 65 Wash.App. 319, 332 [828 P.2d 73, 80], which was overruled in *Waterjet Technology, Inc. v. Flow Intern. Corp.* (2000) 140 Wash.2d 313. *Machen* confuses the "not generally known" requirement with the need to show novelty.

[33] D.22-05-003, p. 47.

2020 WL 9936697, at *10 ("California courts have found a protectable trade secret even if the concept 'might be evident to a [product's] end user.'"). D.22-05-003 faults Lyft for not including in its comments on the Commission's proposed decision the whole of a lengthy quote from *Kewanee,* claiming that

> Lyft has misled the Commission in two material respects: first, it deliberately omitted the language "in the patent sense" between "novelty" and "is not required for a trade secret," thus giving the false impression that novelty is not a requirement for a trade secret claim. Second, Lyft left out the rest of the Supreme Court's comment that "some novelty will be required."

D.22-05-003, p. 105. Lyft firmly, but respectfully, disputes that its failure to cite the entire lengthy passage from *Kewanee* is misleading. As an initial, but not insignificant, matter, Lyft notes that the Commission denied Lyft's request to extend the page limit for comments. As a result, Lyft was severely (and in Lyft's view, unfairly) constrained in attempting to adequately address the errors in the 100-plus page Proposed Decision in only 15 pages, forcing Lyft to radically pare back its case citations to the absolute minimum necessary to preserve its arguments. To then criticize Lyft for not being more expansive is neither reasonable nor fair. More substantively and importantly, the portion of the quote omitted by Lyft – "[h]owever, some novelty will be required, if merely because that which does not possess novelty is usually known"[34] – does ***not*** support a uniqueness requirement, and instead supports precisely what Lyft said in its comments and above; that a trade secret must only "possess at least that modicum of originality which will separate it from everyday knowledge."[35] That is, a trade secret need not be novel or unique – it simply cannot be generally known, and thus common knowledge. The suggestion that because the omitted language mentions the word "novelty," it was misleading to omit it, is simply further confirmation of D.22-05-003's error in mistaking the need for secrecy for a requirement to be unique. Lyft made precisely this point in its Opening Comments on the Proposed Decision, citing to *Phillips*, *infra*,[36] and including the omitted language would have only further served to bolster that point.

---

[34] *Kewanee*, *supra*, 416 U.S. at p. 476.

[35] *Phillips v. Frey*, 20 F.3d 623, 628, 30 U.S.P.Q.2d (BNA) 1755 (5th Cir. 1994).

[36] Comments Of Lyft, Inc. On Proposed Decision Denying Appeal Of Lyft, Inc. Re: Ruling Denying, In Part, Motions By Uber Technologies, Inc. And Lyft, Inc. For Confidential Treatment Of Certain Information In Their 2020 Annual Reports, p. 3.

D.22-05-003 also attempts to distinguish *Altavion, Inc. v. Konica Minolta Systems Lab., Inc.* (2014) 226 Cal.App.4th 26, 54, in which the Court held that "[n]ovelty and invention are not requisite for a trade secret…," by claiming that it was limited only to cases in which prior art is a component of a claim. But *Altavion* simply affirms what *Kewanee*, *Bladeroom*[37] and other courts have held – that a trade secret need not be novel or unique; it must simply not be generally known by those who would make use of it.

It is no surprise that courts would reject the notion that a trade secret must be novel or unique because neither the word "novel" nor "unique" appears in the definition of "trade secret" adopted by the Legislature. Civ. Code, § 3426.1(d). And, in fact, the courts consistently recognize that a proponent need only show independent economic value and reasonable efforts at secrecy. As the court said in *Gartner, Inc. v. Parikh* (C.D. Cal., Oct. 10, 2008, No. CV 07-2039-PSG) 2008 WL 11336333, at *3:

> [T]wo requirements must be met for information to qualify as a trade secret. First, the information must have independent economic value. Cal. Civ. Code § 3426.1(d)(1). Second, the information must be the subject of efforts that are reasonable under the circumstances to maintain its secrecy. Id. at § 3426.1(d)(2)

Id., at *3; *Get Seen Media Group, LLC, et al. v. Orion Tiller, et al. Additional Party Names: Francis Mustafa, LeadVerticals, Inc.* (C.D. Cal., June 23, 2021, No. 220CV11682JAKPDX) 2021 WL 5083741, at *5 ("Under both federal and California law, trade secret protection has two basic requirements: secrecy, and economic value derived from not being known."); *Softketeers, Inc. v. Regal West Corporation* (C.D. Cal., May 6, 2019, No. SACV19519JVSJDEX) 2019 WL 4418819, at *8, *aff'd in part, remanded in part* (9th Cir. 2019) 788 Fed.Appx. 468 ("Trade secret protection has two basic requirements: secrecy, and economic value derived from not being known."). These cases leave no room for the Commission's interjection of a uniqueness requirement found nowhere in the statute.

Compounding the error, D.22-05-003 justifies the failure to consider the evidence Lyft offered in support of trade secret status on the grounds that "once the assigned ALJ determined that Lyft had failed to carry its burden of proof on the first element of a trade secret claim [the

[37] D.22-05-003 also attempts to distinguish *Bladeroom* as limited to expert testimony, but it was not so limited and the fact that the point was made in the context of expert testimony does not alter the fact that a trade secret need not be novel or unique.

erroneous uniqueness or novelty element], it was not necessary for the ALJ to continue and determine if the additional requirements specified in Civil Code § 3426.1(d) for establishing a trade secret claim had been satisfied."[38] The decision in D,22-05-003 not to consider Lyft's evidence on the basis of a nonexistent uniqueness requirement was a further clear error that should not be repeated here.

Finally, even if California law recognized such a requirement – which it does not– as Rosenthal explains, Lyft's Trip Data is entirely unique, as no other company or individual has the ability to assemble the same compilation of data elements concerning rides completed on the Lyft platform.[39] Other companies collect similar data concerning rides on their own platforms, but no one is capable of generating or independently reproducing Lyft's Trip Data. Thus, even if the Commission were correct that California has adopted an unstated uniqueness requirement for trade secrets, it is indisputable that the Trip Data would meet such a requirement and no evidence has even been submitted to contradict that fact.

2. D.22-05-003 Erroneously Found that Lyft Did Not Take Reasonable Efforts to Ensure Secrecy of Its Trip Data

In D.22-05-003, the Commission concluded that Lyft did not demonstrate reasonable efforts to maintain the secrecy of its Trip Data. That determination is clearly erroneous and should be corrected here. The efforts described by Rosenthal are precisely the kind that courts routinely find reasonable. *See, e.g.*, *Religious Technology Center v. Netcom Online*, 923 F.Supp. 1231, 1253 (1995). ("'Reasonable efforts' can include advising employees of the existence of a trade secret, limiting access to the information on a 'need to know basis,' [citation] requiring employees to sign confidentiality agreements, [citation], and keeping secret documents under lock."). D.22-05-003 determined that the measures to which Rosenthal attested in her declaration were insufficient on the grounds that a Lyft driver "knows what zip code from which the proposed ride originates and where it will terminate, and with that information the Lyft driver can determine the census block from where the ride commences and terminates.[40] It goes on to posit that secrecy of the Trip Data is destroyed because of "Lyft's failure to establish that its drivers must sign an exclusivity driving agreement as well as a nondisclosure agreement undermine the trade secret claim since the Lyft

[38] Decision, p. 54; p. 55 (justifying the "Ruling's decision to stop its trade secret analysis after Lyft had failed to satisfy its first evidentiary requirement….").
[39] Rosenthal Decl., ¶ 11.
[40] D.22-05-003, p. 69.

drivers are being provided with unrestrained access to alleged trade secret trip data."[41] However, the courts have long held that compilations are protectable as trade secrets even though individual components are in the public domain.[42] The fact that a particular driver or passenger may have access to select information regarding their own rides (e.g., origination zip code or census block) does not mean the trade secret – *i.e.*, the collection of data elements from millions of rides – has become "generally known." *Religious Technology Center*, 923 F.Supp. 1231, 1255 ("disclosures that describe parts of the works or disclose isolated portions do not necessarily suffice to ruin the value of the entire works as secrets."). As Rosenthal attests, no driver or passenger is given access to data generated by other rides completed on the platform, or to the larger compilation of millions of rides completed over the course of a year.[43]

Materially indistinguishable from the Commission's contention in D.22-05-003, in *San Jose Construction, Inc. v. S.B.C.C., Inc.* (2007) 155 Cal.App.4th 1528, SBCC argued that project binders containing a complete set of bid materials for a construction project could not be trade secret because the bid materials were collected from third party subcontractors, each of whom had access to their own bids and pricing information. The court rejected that argument, explaining that "only SJC had the completed puzzle for each project, contained in the Project Binders.... No third party had it. The subcontractors each had a piece, and the owners had a piece, but no one except SJC had it all." 155 Cal.App.4th 1528, 1539; *see also id.*, at 1542 ("But here, as we have observed, that the binders contained individual components generated by or disclosed to third parties does not mean that the project proposal as a whole was available to each individual contributor."). Likewise here, although an individual driver or passenger has information concerning their own rides, none have all of the pieces which make up the completed puzzle.

The Commission attempted to justify this error by stating that "[w]hat the driver and passenger have unfettered access to is more than the partial disclosures of information in *Religious Technology* and *San Jose Construction*."[44] The Commission cites no record evidence in support of this conclusion, which a careful analysis of the decisions makes clear is simply not accurate. In

---

[41] *Id.*

[42] *See, e.g.*, *Morlife, Inc. v. Perry* (1997) 56 Cal.App.4th 1514, 1522 (customer lists that are not generally available to the public are protected as trade secrets under California law though each customer is aware it is a customer); *Religious Technology Center,* 923 F.Supp. at 1253 (collection of teaching materials protectable as trade secret, even though certain components publicly disclosed); *Mattel*, 782 F.Supp.2d at 972.

[43] Rosenthal Decl., ¶14.

[44] D.22-05-003, p. 113.

San Jose Construction, the trade secret at issue was a collection of bid materials relating to five construction projects. The trial court found "that the binder documents could not have contained trade secrets because all had been either generated by or disclosed to third parties, whether project owners, architects, or subcontractors." *San Jose Construction* 155 Cal.App.4th at 1538. The appellate court reversed, finding that although each bidder had access to their own materials, that did not render the compilation generally known. In *Religious Technology Center*, the defendant argued that the course material "has been largely disclosed in the popular press," in the form of numerous articles discussing certain teaching modules, and that "many of the Advanced Technology documents have been available in open court records in another case." *Religious Technology Center*, 923 F.Supp. at 1255. This was held insufficient to render the compilation generally known. Here, the Trip Data includes a variety of detailed data elements concerning millions of rides completed by millions of individuals over the course of a year, much of which would not be known to either the driver or the passenger, even as to their own rides.[45] The comparatively miniscule sliver of data available to any individual driver or passenger pales in comparison to the core components disclosed in *Religious Technology Center* or *San Jose Construction*. In this regard, it is important to note that Lyft does not claim that the details of any particular ride have independent value. It is the compilation of millions of rides and the patterns and trends which emerge from analysis of that data which has independent value. The fact that any individual driver or passenger has limited information concerning their own rides in no way diminishes the value of the compilation as an analytical tool. That fact is dispositive of the issue and clearly demonstrates the error of D.22-05-003.

3. The Fact that Data Is Required to Be Submitted to the Commission Does Not Strip that Data of Trade Secret Status

The 2020 Ruling affirmed in D.22-05-003 "question[ed] if the trade secret privilege should even be applicable to prevent this public dissemination of any portion of the Annual Reports."[46] Explaining this skepticism, the 2020 Ruling noted that "[i]n D.16-01-014, the Commission found that a common thread between these types of information is that 'it is something that the party claiming a trade secret has created, on its own, to further its business interest,'"[47] and concluded

[45] For example, neither a driver or passenger is likely to know the latitude or longitude of pick up or drop off, the precise number of miles traveled, the census block or census tract, or other fields included in the Trip Data.
[46] ALJ Ruling, p. 15.
[47] *Id.*

that "the mere fact that Moving Parties possess a set of information and group that information for the purposes of complying with a Commission decision or a directive from Commission staff does not transform that information into a trade secret 'compilation.'"[48] Lyft does not contend that the mere fact that data is grouped together for purposes of complying with a Commission directive transforms that data into a trade secret. The pertinent question here is whether the fact that data used by a TNC in the course of its daily operations, and which has enormous commercial value wholly apart from its use in complying with Commission directives, is stripped of its trade secret status by virtue of having to be submitted to the Commission. As explained below, the answer to that question is indisputably "no."

Lyft acknowledges that in D.16-01-014, the Commission suggested TNC trip data might not be a trade secret because it is required to be submitted to the Commission, however, that language is mere *dicta*, as the Commission disposed of trade secret claims on other grounds, and therefore has no precedential value.[49] Second, and perhaps more importantly, the assertion that data required to be submitted to an agency cannot also constitute a trade secret is contrary to law. As stated in *Patel*, regulated entities retain "both a possessory and an ownership interest" in their books and records and have "the right to exclude others from prying into the contents of [those] records…"[50] and those rights are not diminished by "the fact that the records are required to be kept by law."[51] Indeed, the federal Freedom of Information Act, after which the CPRA is modeled,[52] expressly recognizes that data required to be submitted to a regulatory agency may constitute a trade secret, specifically exempting from FOIA's reach "trade secrets and commercial

---

[48] ALJ Ruling, p. 16.

[49] D.16-01-014, Modified Presiding Officer's Decision Finding Raiser-CA, LLC, in Contempt, in Violation of Rule 1.1 of the Commission's Rules of Practice and Procedure, and that Raiser-CA, LLC's License to Operate Should be Suspended for Failure to Comply with Commission Decision 13-09-045,Slip. Op., at 47-48 (Uber failed to show that data would provide competitive advantage); D.20-12-021, p. 32 ("The burden is on the information submitter to prove that the submitted information meets all the elements of the trade secret definition in Civ. Code § 3426.1(d) and that the submitter is entitled to assert the conditional Evid. Code § 1060 trade secret privilege. Neither AT&T, nor Frontier have met that burden with the specificity that GO 66-D requires.").

[50] *Id.* at 1061.

[51] *Id.* at 1062; *McLaughlin v. Kings Island, Div. of Taft Broad. Co.,* 849 F.2d 990, 995–96 (6th Cir.1988) (even in a pervasively regulated industry, that company is required to maintain records does not eliminate "recognizable privacy interest" in those records nor make them "public property."); *Brock v. Emerson Elec. Co.,* 834 F.2d 994, 996 (11th Cir.1987) (fact that records are required by law to be kept "does not serve to strip away a company's attendant privacy interest in that information.").

[52] *City of San Jose v. Superior Court* (2017) 2 Cal.5th 608, 616 ("CPRA was modeled on the federal Freedom of Information Act (FOIA) (5 U.S.C. § 552)"); *San Gabriel Tribune v. Superior Court* (1983) 143 Cal.App.3d 762, 772.

or financial information obtained from a person and privileged or confidential."[53] As the court in *Associated Press v. Federal Bureau of Investigation* explained, confidential trade secret information "required to be submitted to the government" is exempt under 5 U.S.C. §552(b)(4) if disclosure would either impair the government's ability to collect such information, or cause substantial harm to the entity who submitted it.[54] Notably, various states' public access laws which, like the CPRA, were modeled after the FOIA, similarly stipulate that "[a]ny trade secrets obtained from a person or business entity that are required by law, regulation, bid, or request for proposal to be submitted to an agency" are exempt from disclosure.[55] Although the CPRA, unlike the FOIA, does not include an *express* exemption for trade secrets, it is well established that trade secrets are protected under §6254(k) and the California Supreme Court has explained that courts may draw upon FOIA, and judicial decisions interpreting it, in construing the exemptions available under the CPRA.[56] And, of course, California courts have held that use or disclosure of trade secrets by an agency may constitute misappropriation and a Fifth Amendment violation. In *Syngenta Crop Protection, Inc. v. Helliker*, the court analyzed whether data that Syngenta was required to submit to the Department of Pesticide Management as part of its registration application, concerning the health effects and environmental impact of a new pesticide, constituted a trade secret. In ruling on a request for an injunction, the court held that the DPM's use of the data likely constituted unlawful misappropriation of Syngenta's trade secrets, never questioning whether the data was deprived of trade secret status by the fact that the data was required by DPM as part of all new pesticide applications.[57] If, as suggested by the Commission, data required to be submitted to an agency could not constitute a trade secret, the FOIA and state exemptions for trade secrets would be rendered mere surplusage, and the court in *Syngenta Crop Protection* would have simply denied the request for an injunction.

The Commission's suggestion that trip data cannot also constitute a trade secret additionally conflicts with rulings made by other courts which have concluded that TNC trip data does, in fact, constitute a trade secret, although it was collected and submitted for compliance

---

[53] 5 U.S.C. §552(b)(3), §552(b)(4).

[54] *Associated Press v. Federal Bureau of Investigation* (D.D.C. 2017) 265 F.Supp.3d 82, 101.

[55] See, e.g., Ga. Code Ann. § 50-18-72(a)(34); see also Miss. Code. Ann. § 79-23-1 (exempting from public records law "Commercial and financial information of a proprietary nature required to be submitted to a public body").

[56] *San Gabriel Tribune v. Superior Court* (1983) 143 Cal.App.3d 762, 772.

[57] *Syngenta Crop Protection, Inc. v. Helliker* (2006) 138 Cal.App.4th 1135, 1172 (analyzing whether Syngenta met its burden of establishing trade secret status for studies required to be submitted to an agency).

purposes. As noted, in *City of Seattle*,[58] the Supreme Court of the State of Washington affirmed the trial court's determination that even less granular trip data than that at issue here constitutes a trade secret, finding that "the record sufficiently demonstrates the independent economic value of the data reflected by the zip code reports, including as an indicator for potential routes for launching new ride pool and sharing products, and markets for subscription services."[59] The ruling is persuasive authority because both states have adopted the Uniform Trade Secrets Act and employ the same definition of a trade secret.[60]

Here, Lyft has presented sworn testimony that the Trip Data has independent economic value to Lyft, its competitors, and others who could make use of this detailed and highly valuable GPS-derived mobility data, and nothing in the record contradicts such evidence. The fact that some or all of data is also formatted in such a way as to comply with CPED directives and submitted to the Commission in Annual Reports in no way diminishes the uncontradicted evidence that the data has substantial commercial value that would be forever destroyed by the Commission publicly disclosing it.

3. The Commission Has Improperly Determined that Preserving TNC Property Interests Would Work an Injustice

The law protects the trade secrets of private companies from forcible disclosure – and consequent destruction – by regulatory agencies. As stated in *Bridgestone/Firestone, Inc. v. Superior Court* (1992) 7 Cal.App.4th 1384, 1391, *reh'g denied and opinion modified* (July 23, 1992), the government may compel disclosure of a trade secret only where to do otherwise would tend to conceal fraud or work a serious injustice. *See also* Evid. Code §1060 ("[T]he owner of a trade secret has a privilege to refuse to disclose the secret, and to prevent another from disclosing it, if the allowance of the privilege will not tend to conceal fraud or otherwise work injustice."). Indeed, the courts have confirmed that agency use or disclosure of trade secrets may constitute unlawful misappropriation in violation of the California Uniform Trade Secrets Act ("CUTSA"). For example, in *Syngenta Crop Protection, Inc. v. Helliker*, the court held that the Department of Pesticide Management's use of trade secret pesticide data in evaluating applications of a competitor constituted misappropriation of trade secrets, rejecting the DPM's argument that the

[58] 190 Wash. 2d 769 (2018).
[59] *Id*. at 782-83.
[60] *See* RCW 19.108 *et seq.* and Cal. Civil Code §3426 *et seq*.

California Public Records Act ("CPRA") authorized disclosure.[61] Furthermore, as the Supreme Court held in *Ruckelshaus v. Monsanto Co*., agency use of trade secret data of a regulated entity constitutes an unlawful government taking of private property without compensation, in violation of the Fifth Amendment to the Constitution, where the regulated entity has a reasonable, investment-backed expectation of confidentiality.[62] To be sure, as the *Bridgestone/Firestone* court made clear, a narrow exception exists where nondisclosure of the trade secret would conceal fraud or work an injustice; however, in the absence of such a finding, agencies are prohibited by state law and the U.S. Constitution from exposing, and thereby destroying, the trade secrets of entities they regulate.

In D.22-05-003, the Commission correctly acknowledged that the privilege protecting trade secrets may only be overcome if it would conceal fraud or work an injustice, but erroneously held that preservation of TNC trade secrets would work an injustice. The Decision first misstates the burden of proof, holding that "the moving party must prove that the 'allowance of the privilege will not tend to conceal fraud or otherwise work injustice.'"[63] This is incorrect. As stated in *Bridgestone/Firestone*, the burden is on the proponent to establish the existence of a trade secret, however, once established, the burden shifts to the party seeking access to the trade secret to show that nondisclosure would work an injustice. *Id.*, at 1393; *see also Davis v. Leal* (E.D. Cal. 1999) 43 F.Supp.2d 1102, 1110. The Commission attempted to explain this error in D.22-05-003, stating:

> Apparently, Lyft thinks that by "moving party" the Commission is referring to Lyft. It is not. By "moving party," the Commission is referring to the party moving for access to information protected by an established trade secret privilege. As such, "moving party" and "party seeking access" are one in the same so the Commission stands on its earlier analysis as to the allocation of the burden of proof.

D.22-05-003, p. 113-114. Lyft appreciates the effort to clarify what the Commission intended, though it appears to have misspoken. The Commission presumably intended to confirm, consistent with *Bridgestone*, that the party seeking access to the data – and not Lyft – bears the burden of demonstrating that ***nondisclosure would*** work an injustice. Assuming that is what the Commission intended, and consistent therewith, the burden here is upon any party who may

---

[61] *Syngenta Crop Protection, Inc. v. Helliker*, (2006) 138 Cal.App.4th 1135, 1172 (court found such use would improperly "relieve a current applicant of the expense of producing or otherwise acquiring similar data").
[62] *Ruckelshaus v. Monsanto Co.* (1984), 467 U.S. 986, 1004 [104 S.Ct. 2862, 2874, 81 L.Ed.2d 815].
[63] D.22-05-003, p. 72.

oppose this Motion to prove that preserving Lyft's trade secret would conceal fraud or work an injustice. The presumption runs in favor of Lyft; not the other way around.

Equally important, D.22-05-003 fails to acknowledge that under *Bridgestone,* an agency ***must*** consider less intrusive alternatives to public disclosure, including whether a protective order would suffice to prevent injustice. 7 Cal.App.4th at 1393 ("[I]n the balancing process the court must necessarily consider the protection afforded the holder of the privilege by a protective order as well as any less intrusive alternatives to disclosure proposed by the parties."). D.22-05-003 fails to acknowledge this aspect of *Bridgestone*, and otherwise fails to consider whether alternatives exist. The Commission should not repeat that error here.

But perhaps most importantly of all, D.22-05-003 errs in finding that not sharing the data with local governmental agencies would constitute an injustice, citing comments filed by the San Francisco Municipal Transportation Agency ("SFMTA") in this proceeding. But whether the SFMTA would benefit from free access to Lyft's trade secret information is not relevant in determining whether to grant Lyft's request for confidential treatment of its Trip Data. Decisional law makes clear that a desire by local governmental agencies to obtain free access to trade secret data does not qualify as an injustice. In *Bridgestone*, the court held that "[a]llowance of the trade secret privilege may not be deemed to 'work injustice' within the meaning of Evidence Code §1060 simply because it would protect information generally relevant to the subject matter of an action or be helpful to preparation of a case." 7 Cal.App.4th at 1393. In that case, the estate of a woman killed in a car accident arising from the defendant's tire sought disclosure of the chemical formula used in manufacturing on the grounds that it would assist the plaintiff's expert in establishing why the tire failed. The court held that to overcome the trade secret claim, plaintiff must prove that the formula was both "relevant and necessary" to her claim and "essential to a fair resolution of the lawsuit." *Id.*, at 1393. Although plaintiff's expert "gave specific examples of the manner in which formulas were helpful in evaluating the reasons why tire components fail," and "explained, from his own experience and that of others in the field, how information like that sought by real parties was important in an analysis and proof of why a tire failed," the court refused to order disclosure, finding that access to the formula was not essential to that analysis. *Id.*, at 1396-97. This bears repeating: although the tire formula was concededly instrumental to assessment of liability for the death of the plaintiff, the court nevertheless refused to order its disclosure. A desire by local agencies to have access to TNC data for planning purposes, as to

which they concededly have alternatives, does not come close to meeting the standard established in *Bridgestone*.

In the few cases where courts have found injustice, the courts have imposed a very high bar. In *State Farm Fire & Casualty Co. v. Superior Court* (1997) 54 Cal.App.4th 625, 651, *as modified* (May 1, 1997), the court so held only because the crime-fraud exception vitiated both the attorney client privilege and the trade secret privilege, and the trade secret was essential to the dispute. That is not so as to Trip Data. In *Uribe v. Howie* (1971) 19 Cal.App.3d 194, the court declined to allow concealment of the composition of pesticide sprays because the information was necessary to "study the long range effects of pesticides on humans, and in the treatment of present illnesses traceable in whole or part to exposure to these chemicals." *Id.*, at 210. Thus, only because the data was necessary to preserve human health was it appropriate to require disclosure.

In D.22-05-003, the Commission conceded that TNC Trip Data is not essential. As stated in party comments, local governmental agencies have access to alternative data but would prefer to have the Commission seize Lyft's Trip Data and turn it over to them at no cost. The 2020 Ruling, which D.22-05-003 affirms, quotes SFMTA's admission that "[w]ithout TNC data, SFMTA transportation planners must rely instead on anecdotal information to fill the gap," and that "[c]reating public policy on factual, real time data, is clearly preferable."[64] San Francisco expressly concedes that it has alternate sources to TNC transportation data. The San Francisco County Transportation Authority ("SFCTA") prepared a highly detailed analysis of the impact of TNCs in San Francisco in 2018, called "TNCs and Congestion,"[65] in which SFCTA explained that it gathered data from a variety of sources, including data concerning "observed roadway conditions … derived using the GPS- and fleet-based speed data licensed from [a company called] INRIX,"[66] as well as "San Francisco's travel demand model, SF-CHAMP, [which] produces estimates of traffic volumes on all roads in San Francisco and requires inputs describing factors such as population, employment, and multi-modal transportation network capacity and performance."[67] Although SFCTA admits it could access alternative sources of data, it made clear that it did not

---

[64] 2020 Ruling, p. 57.

[65] Opening Comments of the San Francisco Municipal Transportation Agency, San Francisco County Transportation Authority, San Francisco City Attorney's Office, and San Francisco International Airport To Phase III.C Scoping Memo And Ruling Of Assigned Commissioner: Track 3 – TNC Data ("SF III.C Comments") p. 10; TNCs and Congestion, at https://www.sfcta.org/sites/default/files/2019-05/TNCs_Congestion_Report_181015_Finals.pdf

[66] *See* TNCs and Congestion, p. 13, for a detailed description of the data obtained by SFTCA.

[67] *Id.*, p. 14.

think it should have to pay for the data, stating that "[t]he veil created by footnote 42 forced the TA to allocate hundreds of professional staff hours and tens of thousands of dollars to find alternative sources of data to inform its recent analysis of the impact of TNC service on traffic congestion in San Francisco."[68] As shown in *Bridgestone*, *State Farm* and *Howie,* however, the mere fact that local agencies could save some time and effort by having the Commission confiscate TNC Trip Data is patently insufficient to constitute an injustice.

Even more concerning, D.22-05-003 also attempts to bolster its finding concerning an injustice by citing *City and County of San Francisco v. Uber Technologies, Inc.* (2019) 36 Cal.App.5th 66, 73-74 for the proposition that "a municipality's interest in obtaining a TNC's trip data goes beyond environmental and infrastructure matters."[69] However, that decision merely illustrates the 2020 Ruling's dangerous implications. In *Uber Technologies, Inc.*, the City Attorney issued administrative subpoenas demanding that Uber produce Annual Reports, and Uber objected arguing production would impinge on the privacy of users and Uber's trade secrets. The court held the City Attorney "has a broad right to investigate, including the use of subpoenas, when it suspects an entity operating within its jurisdiction is violating the law" and that "[t]he subpoenaed items are relevant to an investigation of possible violations of law." 36 Cal.App.5th 66, 73–74, 75. Contrary to the Commission's suggestion in D.22-05-003, the court did ***not*** find that Uber's Annual Reports should be publicly disclosed. Instead, the court ***acknowledged*** Uber's confidentiality interests and held that those interests could be preserved by a stipulated protective order which ***expressly required*** the city to withhold the Annual Reports under the CPRA. *Id.*, at 83. Thus, the opinion upon which the Commission relies to justify its decision directly contradicts the Commission's decision.

Worse still, D.22-05-003 goes on to assert that "[s]everal investigations into whether a TNC like Lyft is operating in violation of various state and local laws would be stymied if governmental entities could not review the relevant trip data. Accordingly, assuming that the trip data was a trade secret, keeping that trip data private is outweighed by the injustice inflicted on governmental entities who would be denied access to trip data."[70] That is, D.22-05-003 holds that although municipalities may obtain TNC data in support of a legitimate investigation into criminal

[68] SF III.C Comments, p. 10.
[69] PD, pp. 74-76.
[70] D.22-05-003, p. 76.

or regulatory violations, an injustice would be "inflicted" upon them if they were not allowed to circumvent the due process limitations imposed on administrative or other subpoenas,[71] or had to agree to protect trade secrets under a protective order. In *Carpenter v. U.S.* (2018) 138 S.Ct. 2206, the Supreme Court warned against precisely this concern – warrantless fishing expeditions by law enforcement into a database of vehicle location data collected by a private company. *Id.* at 2218. The contention that Lyft's Trip Data must be disclosed for use by governmental entities in warrantless fishing expeditions in search of potential wrongdoing is contrary to law, including fundamental constitutional rights, and truly ominous in its implications.

Lyft has demonstrated that the Trip Data has economic value from not being generally known and is the subject to reasonable efforts to maintain its secrecy, and no party has established, or can establish, that preservation of Lyft's trade secret would work an injustice.

C. The Trip Data Is Also Protected under § 6254(c) as Files the Disclosure of which Would Constitute an Unwarranted Invasion of Privacy

The California Constitution expressly provides that "nothing" about the right of the people to access "writings of public officials… supersedes or modifies the right of privacy guaranteed by Section 1."[72] Thus, the Supreme Court recently cautioned "that increased public access to government records can come at the expense of personal privacy and other important confidentiality interests."[73] Government Code § 6254(c), among other provisions, was enacted for the purpose of ensuring that agencies responding to requests for access do not infringe upon the privacy rights of individuals to whom the information relates.[74] Importantly, if submission of data to a government agency vitiated the privacy rights of the submitting party, there would be no need for § 6254(c), as there would be no continuing privacy right to protect.

1. Disclosing Trip Data at the Census Block and Zip Code Level Does Not Prevent Identification of Specific Individuals

The 2020 Ruling agreed that to the extent TNC trip data includes driver names, vehicle identification numbers, and precise latitude and longitude data, that data is protected from disclosure pursuant to §6254(c), correctly finding "support for the proposition that this information

---

[71] *City and County of San Francisco v. Uber Technologies, Inc.* (2019) 36 Cal.App.5th 66, 74 (administrative subpoena must (1) relate to an inquiry which the administrative agency is authorized to make; (2) seek information reasonably relevant to that inquiry; and (3) not be too indefinite).

[72] Cal. Const., Art. I, §3(b)(3).

[73] *National Lawyers Guild , San Francisco Bay Area Chapter v. City of Hayward* (2020) 9 Cal.5th 488, 492–493.

[74] *Id*. at 493.

might be engineered to identify the exact starting and ending addresses of a trip, which can then be combined with other information to identify a driver and/or passenger."[75] The 2020 Ruling rejected confidential treatment for "the balance of the geolocational data (date and time, census block and zip code of both the driver and rider; when the rider is picked up and dropped off; when the driver's app is turned on or the last rider dropped off; time a trip request was made; and when the trip request was accepted on the TNC's app)."[76] The 2020 Ruling found that Lyft and Uber "failed to make the necessary granular showing" to support confidential treatment.[77]

Lyft supports the Ruling's determination to protect driver details, vehicle and license numbers, and precise latitude and longitude data, and does not dispute that redaction of such fields reduces the risk of re-identification of TNC trip data. However, the balance of the Trip Data also includes a wealth of information concerning millions of rides completed on the Lyft platform over the preceding year, including the precise date and time of pick-up and drop-off, and the location of the requester, pick-up location of the passenger, and drop off location of the passenger, by zip code and census block, as well as the miles traveled. As explained below, mobility data of precisely this level of granularity can be readily used to identify specific individuals and track their movements, potentially revealing intimate personal details, such as medical visits, political affiliations, personal relationships, sexual orientation, etc.

As the US Census Bureau explains, the census block is the "smallest level of geography you can get basic demographic data for, such as total population by age, sex, and race" and is "[g]enerally small in area. In a city, a census block looks like a city block bounded on all sides by streets."[78] Indeed, as the Census Bureau vividly illustrates in the presentation attached as Exhibit A hereto, a census block may include as few as ***five*** individuals.[79] In her declaration, Rosenthal explains that the Census Office of the State of California has created an interactive map that identifies census tracts and census blocks within California, along with a variety of statistics and

---

[75] 2020 Ruling, p. 5.
[76] *Id.*
[77] *Id.*
[78] https://www.census.gov/newsroom/blogs/random-samplings/2011/07/what-are-census-blocks.html Lyft requests official notice of this document by the Census Bureau pursuant to Evid. Code § 452(c) and § 452(h), and Rule of Pract. and Proc. 13.10.
[79] Rosenthal Decl., Exhibit A, slide 9. Lyft requests official notice of this document by the Census Bureau pursuant to Evid. Code § 452(c) and § 452(h), and Rule of Pract. and Proc. 13.10.

demographic information related to such blocks and tracts.[80] The map can be found at https://census.ca.gov/htc-map/.[81] The map itself is located at https://cacensus.maps.arcgis.com/apps/webappviewer/index.html?id=48be59de0ba94a3dacff1c9116df8b37.[82] Each census tract and block is assigned a unique GEOID.[83] The Census Office map allows users to isolate each census block and to examine various statistics and demographic information.[84] The map reveals that California has numerous census blocks which include only a handful of individuals.

For example, Census Bloc GEOID 06059021813, in Placentia, California – in Orange County and only six miles from Anaheim – has a population of three individuals.[85] Census Block GEOID 06037980009, located in Los Angeles halfway between Hollywood and Glendale, has a population of five individuals.[86] Census Block GEOID 06037980034, in Los Angeles County, near Buena Park, has a population of nine individuals.[87] Census Block GEOID 06083980500, in Santa Barbara County, just north of the Vandenburg Airforce base, has a population of nineteen individuals.[88] Census Block GEOID 06001982000, in Alameda, has a population of twenty-six individuals.[89] Census Block GEOID 06075980300, in San Francisco, has a population of thirty-two individuals.[90] As Rosenthal attests, Lyft's rideshare service is available in each of these census blocks.[91] The foregoing are examples of census blocks with few individuals, but there are many other census blocks with only a handful of individuals who live there.[92]

In census blocks with a small number of individuals, mobility data on the census block level provides little or no opportunity for anonymity, and makes the tracking of individuals'

---

[80] Rosenthal Decl., ¶19. Lyft requests official notice of the California Census Office website, the interactive map, and the data contained therein (some of which is set forth in Exhibits B – G to Rosenthal's Declaration) pursuant to Evid. Code § 452(c) and § 452(h), and Rule of Pract. and Proc. 13.10

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] Rosenthal Decl., Exhibit C.

[86] Rosenthal Decl., Exhibit D.

[87] Rosenthal Decl., Exhibit E.

[88] Rosenthal Decl., Exhibit F.

[89] Rosenthal Decl., Exhibit G.

[90] Rosenthal Decl., Exhibit H.

[91] Rosenthal Decl., ¶ 20.

[92] *Id.*

movement quite easy. By sorting the Trip Data by census block, one can identify every trip made by one of the few individuals who live in these census blocks. With a only a modicum of additional information, one can rather easily identify specific individuals living within these census blocks and track their movements over the course of a year – or many years as time goes on. In the 2020 Ruling affirmed in D.22-05-003, the Commission "agree[d] with Moving Parties with respect to the latitude and longitude of both the driver and rider of a particular TNC trip" finding "[s]upport for the proposition that this information might be engineered to identify the exact starting and ending addresses of a trip, which can then be combined with other information to identify a driver and/or passenger."[93] Having found that latitude and longitude information might be combined with other information to identify specific individuals, the Commission must also acknowledge that disclosing census blocks, many of which have few individuals, could similarly allow for the identification of specific individuals, in violation of the right to privacy implicitly recognized by the 2020 Ruling.

Furthermore, although the above-cited census blocks present a particularly compelling demonstration of the lack of anonymity provided by census block reporting, it must also be acknowledged that even densely populated city blocks implicate similar privacy concerns. Consider the revealing information one can learn with just a few details regarding an individual and the time and location at which a ride commenced. An individual standing on a street corner in his San Francisco neighborhood who happens to see his neighbor get into a Lyft or Uber could, by reference to the Trip Data, ascertain the person's destination by simply sorting the data by date, time and census block; whether to her office located in one census block or zip code, to a suspected paramour's residence, to a healthcare or psychiatric facility, to an AIDS clinic, to a political rally, or to another suspected location known to be in a different census block or zip code. Indeed, given the modern day ubiquity of third party surveillance video outside many office and apartment buildings, restaurants, private residences, and other locations in densely populated cities, one would not need to be standing on a street corner to acquire the information necessary to identify a specific individual and track their movements, as the combination of the video and the Trip Data would effectively create a persistent historical record of the data necessary to do so. Likewise, using a combination of surveillance video and Trip Data, law enforcement could

[93] 2020 Ruling, p. 5.

effectively travel back in time to ascertain an individual's whereabouts without the necessity of obtaining a warrant or otherwise gaining lawful access to geolocation data for a suspect. As the above examples illustrate, with only a few additional details, acquiring private and personally revealing information regarding specific individuals is a rather rudimentary exercise, even without knowledge of advanced data re-identification techniques. Put simply, the Commission can provide no assurances to the TNC-using public that such a massive, detailed, and content-rich database will not be misused for a variety of nefarious purposes. Ordering that such data be publicly disclosed in the absence of such assurances is exceedingly unwise.

Confirming the foregoing, the Census Bureau openly acknowledges the privacy implications of publicly disclosing data at the census block level, sharply limiting the data it will release that is linked to census block, even as to researchers who may gain access only for limited approved uses and subject to contractual restrictions on dissemination.[94] In fact, for the 2020 Census, the Census Bureau embarked on a massive Disclosure Avoidance Modernization project with assistance from leading experts on data anonymization to ensure that its data cannot be re-identified to expose private details regarding individuals.[95] It is highly unlikely that the Census Bureau would undertake such a costly and time-consuming effort to anonymize its data if data at the census block level did not implicate serious personal privacy concerns.

The Federal Trade Commission has also recognized that it is not merely precise latitude and longitude coordinates that constitute sensitive personal information. The FTC considers any "geolocation information sufficient to identify street name and name of a city or town" to be sensitive and subject to restrictions on collection.[96] As the Director of the Federal Trade Commission's Bureau of Consumer Protection testified before Congress:

> Geolocation information can divulge intimately personal details about an individual. Did you visit an AIDS clinic last Tuesday?

---

[94] Univ. of Michigan, Inst. For Social Research, Panel Study of Income Dynamics ("Because particular Census Blocks may consist of small populations, the Census makes available relatively few variables to which Census Block can be linked.") at https://simba.isr.umich.edu/restricted/Geospatial.aspx#:~:text=Block%2DGroup%3A%20A%20higher%20level,area)%20called%20Block%2DGroup.&text=For%20example%2C%20for%20Census%202000,numbered%20from%203000%20to%203999. Lyft requests official notice of this study pursuant to Evid. Code § 452(h).

[95] https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance.html Lyft requests official notice of the US Census Bureau documents cited herein pursuant to Evid. Code § 452(c) (official acts) and § 452(h) (facts subject to verification by reference to sources of reasonably indisputable accuracy).

[96] 16 C.F.R. § 312.2.

> What place of worship do you attend? Were you at a psychiatrist's office last week? Did you meet with a prospective business customer?"[97]

Numerous academic studies have also shown that similarly granular data can be reverse-engineered to identify individuals and track their movements. For example, a study involving the inadvertent release of New York City taxi data, which included time and generalized pick up location, as well as an anonymized license number, found that the data allowed researchers to track the movements of individual drivers and passengers.[98] Other studies have found that mobility data of various types can be used to identify individuals and that 95% of individuals can be identified using only four spatio-temporal data points.[99] As noted above, the Trip Data includes far more than four spatio-temporal data points; e.g., date, time, zip code, and census block for the trip request and passenger pick up and drop off, as well as miles traveled, over the span of a year and millions of individuals trips.

Although the 2020 Ruling ordered that latitude and longitude be redacted, other studies show that this does ***not*** eliminate the risk of re-identification. For example, a paper entitled *The Tradeoff between the Utility and Risk of Location Data and Implications for Public Good* found that even geolocation data aggregated to the census block level presents a serious risk of de-identification.[100] As the study explained:

> Mere observation of this data reveals the movements of individuals between neighborhoods. With simple tooling, mobility data at this resolution is detailed enough to describe traffic flows, geographic areas that an individual frequents, and a person's daily routines [citation]. [Cell Data Records] with this type of location data have been used in machine learning models to correctly infer the

---

[97] https://www.ftc.gov/news-events/press-releases/2014/06/ftc-testifies-geolocation-privacy. Lyft requests official notice of the FTC Director's testimony pursuant to Evid. Code § 452 (c) and (h).

[98] Motion, p. 27, fn 145.

[99] See Id. at fn. 146; see also "Spatio-temporal techniques for user identification by means of GPS mobility data," Luca Rossi, James Walker & Mirco Musolesi, EPJ Data Science volume 4, Article number: 11 (2015) at https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-015-0049-x (analyzing CabSpot data on taxi cabs and concluding that "When the full-resolution 5 digits GPS coordinates are used, we have that in both the CabSpot-ting and the CenceMe datasets as little as two points are sufficient to uniquely identify nearly 100% of the individuals…. Remarkably, we see that the number of points in P plays a fundamental role in the determination of the level of uniqueness in the CabSpotting dataset. Here increasing the number of points to 3 or more raises the uniqueness to 100%, regardless of the number of users in the dataset."). Lyft requests official notice pursuant to § 452(g).

[100] Rosenthal Decl., ¶ 22. *See* https://arxiv.org/pdf/1905.09350.pdf for study.

> professions and unemployment status of individuals, as well as other socio economic characteristics.[101]

As the authors explain, "[t]his data no longer reports people's precise locations, making it more difficult to infer home addresses or the sensitive places they may have visited[, h]owever, understanding the daily mobility traces of individuals still provides valuable information to skip-tracing firms and law enforcement agencies … to track suspects' movements and using their locations to implicate them at the time of trial has become common."[102] The study further finds that even when census block data is fully aggregated, "with advanced methods, the likely trajectories of neighborhood residents can be estimated" and "[r]ecent research has shown that in ideal scenarios, user trajectories can be recovered with up to 91% accuracy from aggregated location data that was collected from mobile applications."[103] The study ultimately concludes that the "[t]he re-identifiability risk in this data is high."[104]

Similar concerns have been expressed regarding the release of data by zip code.[105] This is not surprising. As of the 2010 census, California had thirty-six zip codes with fewer than one-hundred residents and eighty-three zip codes with fewer than two-hundred residents.[106] By comparison, rules adopted to implement the Health Insurance Portability and Accountability Act (HIPAA) recognize that where data is linked to zip codes with fewer than 20,000 residents, additional de-identification measures must be taken to prevent re-identification of medical data.[107] Courts have also held that a consumer's zip code constitutes personally identifiable information.[108] And, as explained above, rich datasets which include numerous spatio-temporal data points,

---

[101] Id. at p. 10.
[102] *Id.* at p. 11.
[103] *Id.* at p. 13.
[104] Id. at p. 11.
[105] "Do Data Releases Based on ZIP Codes Endanger Patient Privacy?" at https://www.govtech.com/health/releasing-covid-19-case-numbers-in-zip-codes-may-violate-patient-privacy.html; "Open Police Data Re-identification Risks," Lorrie Cranor, FTC Chief Technologist, at https://www.ftc.gov/news-events/blogs/techftc/2016/04/open-police-data-re-identification-risks (zip codes with homogeneous populations present higher risks of re-identification for heterogeneous residents). Lyft requests official notice pursuant to §452(c) and (g).
[106] https://www.california-demographics.com/zip_codes_by_population.
[107] 45 CCR §164.514 (de-identification safe harbor requires masking zip code for zip codes with fewer than 20,000 people); "Simple Demographics Often Identify People Uniquely," (individuals can be identified with only zip code, gender and age) at https://dataprivacylab.org/projects/identifiability/paper1.pdf
[108] *Pineda v. Williams-Sonoma Stores, Inc.* (2011) 51 Cal.4th 524, 531; *Tyler v. Michaels Stores, Inc*. (2013) 464 Mass. 492, 506 ("a zip code constitutes personal identification information").

particularly over time, allow for ready re-identification of individuals and their movements, even without precise geolocation coordinates.

The 2020 Ruling acknowledges that "Moving Parties also cite to a series of research papers and reports showing the manipulation of that anonymized data sets can, with a high probability, reveal individual identifications," but dismisses those studies on the grounds that Lyft and Uber "fail to demonstrate that any of these research papers and reports used the same geolocational data that Moving Parties must provide in an unredacted form."[109] However, as the MIT study cited above makes clear,[110] it is cell-phone derived mobility data that presents privacy implications. The precise manner in which such mobility data is collected – whether by a Lyft app, a Google app, a Facebook app or a vehicle's internal GPS system-- is irrelevant and offers no basis to conclude that re-identifying TNC mobility would be significantly more difficult.

2. The Courts Have Expressly Acknowledged the Dangers of Allowing Unfettered Access to Data Which Can Be Reverse-Engineered to Identify Specific Individuals

In D.22-05-003, the Commission implicitly holds that disclosure of Trip Data at the census block and zip code level does not implicate user privacy concerns. As shown above, however, merely redacting latitude and longitude does not prevent re-identification, and the courts have made clear that data that is capable of re-identification implicates the constitutional right of privacy. For example, in *Sander v. Superior Court,* 26 Cal. App. 5th 651 (2018), a researcher sought to compel the State Bar to produce "individually ***un***identifiable records for all applicants to the California Bar Examination from 1972 to 2008 in the following categories: race or ethnicity, law school, transfer status, year of law school graduation, law school and … GPA, LSAT scores, and performance on the bar examination." *Id.*, at 658 (emphasis added). Plaintiffs sought no names, addresses or other personally identifiable information and argued that "making these records available to the public in a manner that protects the applicants' privacy and anonymity" would allow study of bar passage rates between racial and ethnic groups. The State Bar refused, saying the data might be re-identified. Although plaintiffs proposed various de-identification protocols, the Court of Appeal upheld the State Bar's refusal, affirming the determination that

[109] Id., at pp. 5-6.
[110] https://arxiv.org/pdf/1905.09350.pdf

"individual applicants may be identified from the data" and further holding that the CPRA does not require manipulation of data to prevent re-identification. *Id.* at 665.

In *Carpenter*, the Supreme Court likewise warned of the dangerous consequences of allowing access even to coarse location data where the data chronicles an individual's movements over time. At issue was whether the defendant had a reasonable expectation of privacy in Cell-Site Location Information ("CSLI") collected by a mobile carrier. The Court explained that even where data is collected by "leverag[ing] the technology of a wireless carrier,… an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Id*. The Court rejected the government's contention that CSLI presented no privacy concerns because it is "less precise than GPS information" and sufficient only to place the defendant "within a wedge-shaped sector ranging from one-eighth to four square miles" – essentially the same as a census block – but the Court disagreed, "reject[ing] the proposition that 'inference insulates a search'" and noting that "[f]rom the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements,…" *Id.* at 2218. "[T]he time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations." *Carpenter*, at 2217. Most ominously, the Court explained:

> [T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers…. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone…. [P]olice need not even know in advance whether they want to follow a particular individual, or when. Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years.

138 S.Ct. 2206, 2218. The same concerns expressed by the Supreme Court in *Carpenter* and *Sander* are presented here. Public disclosure of a massive database of historical location data concerning the movements of the millions of people who used Lyft in California 2020 would allow

anyone to essentially travel back in time to reveal intimate details of their lives. Lyft respectfully submits that such a decision would have profound, negative reverberations for users of TNCs in California, without soliciting any input from those users as to whether they want their data released.

The evidence presented by Lyft shows that the Trip Data pinpoints location to an area the size of a city block,[111] materially indistinguishable from the CLSI at issue in *Carpenter*, which discloses a wedge shaped area between an 1/8 and four square miles. Thus, although the Trip Data does not itself identify individuals, it presents a serious risk of re-identification— just like the data in *Sander* and the lat/long data D.22-05-003 agreed to protect. And like the data in *Carpenter*, the retrospective quality of the Trip Data would, in effect, create a massive and permanent historical record of the ***every*** Lyft trip taken by anyone in California, and as with the CLSI in *Carpenter*, once disclosed, it would represent precisely the historical repository of mobility data that the Supreme Court feared. It requires no stretch of the imagination to envision that once produced, a massive historical database of time-stamped records of every ride completed by TNCs in California could be mined by law enforcement, jilted ex-lovers, jealous spouses, and others for myriad purposes, both benign and nefarious. No one – the Commission included – can predict how such data might be used, and once released, there is no clawing it back. The Commission should grant Lyft's request for confidential treatment of its Trip Data.

D. D.22-05-003 Errs in Failing to Even Acknowledge Lyft's Constitutional Right to Privacy

As explained above, the Supreme Court recently affirmed that even closely regulated entities, such as TNCs, retain a constitutionally protected right of privacy in the data collected in the course of their operations. *See Patel*, 738 F.3d at 1061-1062; *City of Los Angeles, Calif. v. Patel* (2015) 576 U.S. 409, 426 (affirming). The expectation of privacy recognized in *Patel* extends to internet-enabled platforms such as Lyft. *Airbnb, Inc. v. City of New York*, 373 F. Supp. 3d 467; *Airbnb, Inc. v. City of Boston,* 386 F.Supp.3d 113, 125 ("Airbnb has a reasonable expectation of privacy in the nonpublic usage data for its listings—especially when paired with additional information such as the location of the unit…"). So too here, Lyft has compelling

[111] https://www.census.gov/newsroom/blogs/random-samplings/2011/07/what-are-census-blocks.html; Rosenthal Decl., Exhibit A.

reasons to maintain the confidentiality of its data – both to preserve its competitive position and to promote its relationship with its users by maintaining their privacy.

D.22-05-003 dismissed the *Airbnb* decisions by claiming that because specific names and addresses are not disclosed, the decisions are distinguishable. But those decisions are clear that the property right at issue is Lyft's, not that of its users, and that right in no way depends upon the granularity of the data disclosed. Furthermore, as shown in *Carpenter* and *Sander,* even coarse data implicates constitutionally protected rights where it might be re-identified. Before ordering the disclosure of Lyft's Trip Data, the Commission is required to acknowledge Lyft's constitutionally protected interest in nondisclosure of its data and establish a lawful basis for violating that interest.

E. The Commission Should Allow Redaction of Vehicle Make, Model, and Year from the Assault and Harassment Report for the Same Reasons Identified in the Confidentiality Ruling as to That Report

In addition to the Trip Data for which Lyft seeks confidential treatment, Lyft also seeks confidential treatment of the following fields in the report entitled Assaults and Harassment: Vehicle Make; Vehicle Model; and Vehicle Year. The 2020 Ruling found that the following fields may be redacted from the Assaults and Harassment Report on the grounds the disclosure would implicate a significant privacy interest: Waybill ID; DriverID; VIN; AssaultHarassLat; AssaultHarassLong; AssaultHarassType; AssaultHarassDef; AssaultHarassDescr. Lyft believes that the fields for Vehicle Make, Vehicle Model, and Vehicle Year should be treated confidentially for the same reason. Although in the vast majority of instances, disclosure of the make, model, and year would not allow a third party to identify a particular owner of a vehicle, there may be instances in which disclosure of these fields might allow identification of a particular individual, including the fact that the individual was subject to an unverified and unsubstantiated allegation of harassment or sexual assault or the victim of such an actual assault; for instance, where a particularly unique or rare vehicle model or year is involved. Furthermore, there is no substantial public interest in disclosing this information. Thus, these fields should be protected from disclosure pursuant to Government Code §6254(c), as a file the disclosure of which would constitute an unwarranted invasion of privacy, § 6254(k) and the Right of Privacy guaranteed by Article I, Sect. 1, of the California Constitution, and the public interest exception of Government Code §6255, in that the public interest in disclosure is significantly outweighed by the privacy implications of disclosure.

F. Lyft's Evidence Is Not Inadmissible on Hearsay Grounds or For Lack of Authentication

Both the 2020 Ruling and D.22-05-003 refused to consider Lyft's evidence by variously claiming either that it was inadmissible hearsay or lacked authentication, and then, having excluded Lyft's evidence, declared that Lyft had unsurprisingly failed to carry its evidentiary burden. Lyft had submitted, and also proffers here, a variety of evidence, including: (1) US Health and Human Services administration regulations; (2) Congressional testimony of the Director of the Federal Trade Commission's Bureau of Consumer Protection; (3) official publications of the United States Census Bureau describing census blocks and the Bureau's Disclosure Avoidance Modernization project (designed to minimize the privacy risk of disclosing census-block level data); and (4) academic studies, including one by Massachusetts Institute of Technology data scientists entitled "The Tradeoff Between the Utility and Risk of Location Data and Implications for Public Good,"[112] speaking directly to the risks of disclosing mobility data at the level of granularity proposed by the 2020 Ruling and D.22-05-003. D.22-05-003 dismissed all of this evidence as "inadmissible hearsay" and questioned why Lyft "did not follow the procedure of procuring declarations under oath to support their conclusions, or why declarations were not secured from the authors of the testimony, paper, and Health Insurance Portability and Accountability Act rules and submitted along with Lyft's Motion."[113] As explained below, D.22-05-003 misconstrued the hearsay rule and contravened the Commission's own rules and precedent. In so doing, it resulted in a denial of due process. *App. of Pac. Gas & Elec. Co. for 2013 Rate Design Window Proceeding (U39e)* (June 11, 2015) 2015 WL 3879847, *12 ("It would be unlawful for the Commission to entirely exclude evidence on one side touching on an essential matter at issue, as this would amount to a denial of due process of law.").

First, reliance on the hearsay rule to exclude evidence is directly inconsistent with D.20-03-014, which created a "new protocol" that requires submissions of only a declaration and allows no hearing, leaving TNCs with ***no choice but to rely upon hearsay***. Hearsay is any "statement that was made other than by a witness while testifying at the hearing and that is offered to prove the truth of the matter stated." Evid. Code § 1200. Because D.20-03-014 does not allow for a hearing, any evidence offered for its truth in support of confidential treatment is hearsay. In fact, D.20-03-

[112] 2021 Motion, pp. 28-31.
[113] D.22-05-003, p. 97.

014 expressly ***requires*** that TNCs rely on hearsay, by requiring a written declaration, which is itself a classic form of hearsay. *Rushing v. Neuschmid* (N.D. Cal., May 12, 2020, No. 18-CV-02351-BLF) 2020 WL 2404666, at *33, citing *In re Fields*, 51 Cal. 3d 1063, 1070 (1990) ("[A]n out-of-court declaration is hearsay,…"); *Fortune v. Fortune* (Fla. Dist. Ct. App. 2011) 61 So.3d 441, 445 ("The affidavit, an out-of-court statement offered to prove the truth of the matter asserted, is the most basic form of hearsay.").

D.22-05-003's rejection of Lyft's evidence as hearsay also contradicts longstanding Commission precedent and the Commission's own Rules of Practice and Procedure, which recognize that "hearsay evidence is admissible in Commission proceedings…." D.99-01-029, 84 CPUC 2d 698 (Jan. 20, 1999); D.99-01-029 (accepting into evidence a form submitted to the Securities Exchange Commission and explaining "[t]he Commission generally allows hearsay evidence if a responsible person would rely upon it in the conduct of serious affairs."); *see also The Utility Reform Network v. Public Utilities Com*. (2014) 223 Cal.App.4th 945, 959–960 ("The Commission's own precedent establishes that hearsay evidence is admissible in its proceedings.").

D.22-05-003 also fails to recognize that much of the evidence offered by Lyft and identified as "inadmissible hearsay" is not hearsay at all, as it is not submitted for the truth of the matter asserted. *People v. Turner* (1994) 8 Cal.4th 137 ("[A]n out-of-court statement is admissible if offered for a nonhearsay purpose—that is, for something other than the truth of the matter asserted—and the nonhearsay purpose is relevant to an issue in dispute."). The evidence cited above is submitted not for the truth of any particular statement asserted therein but as circumstantial evidence of the privacy implications of releasing even granular location data. Additionally, even if certain evidence did constitute hearsay, numerous exceptions are recognized; for example, where indicia of trustworthiness are present or where the veracity of the declarant is of less concern. *People v. Cudjo* (1993) 6 Cal.4th 585, 608, *as modified on denial of reh'g* (Feb. 9, 1994) ("Because the rule excluding hearsay is based on these particular difficulties in assessing the credibility of statements made outside the jury's presence, the focus of the rule's several exceptions is also on the reliability of the out-of-court declaration. Thus, the various hearsay exceptions generally reflect situations in which circumstances affording some assurance of trustworthiness compensate for the absence of the oath, cross-examination, and jury observation."). D.22-05-003 simply declared all of Lyft's evidence "inadmissible hearsay," without analyzing the evidence, the purpose for which it was submitted, and whether it falls within a recognized exception.

For example, D.22-05-003 refuses to consider duly promulgated federal regulations, going so far as to fault Lyft for not obtaining a declaration from the "author" of the "Health Insurance Portability and Accountability Act rules."[114] It cannot seriously be maintained that Lyft must obtain a sworn declaration from the Secretary of the Department of Health and Human Services in order to have the Commission consider federal HIPAA regulations. In any event, the rules are not even hearsay, as they are not offered for the truth of any assertion therein, but as circumstantial evidence of the federal government's concern that even data aggregated at a level far beyond what is contemplated here carries a significant risk of re-identification. Nor are the official publications of the US Census Bureau, which provide statistics on census block population and describe the Bureau's 2020 Disclosure Avoidance Modernization project, inadmissible hearsay. They are official US government publications and thus constitute non-hearsay public records under both state and federal law.[115] A finder of fact is entitled to presume that a public report is authentic and trustworthy, as public officials are presumed to perform their duties properly without motive or interest other than to submit accurate and fair reports. *See Gilbrook v. City of Westminster,* 177 F.3d 839, 858 (9th Cir. 1999); *Johnson v. City of Pleasanton,* 982 F.2d 350, 352 (9th Cir. 1992). As a result, cross-examination is unnecessary to test their credibility. *Ibid*. Furthermore, the Census Bureau records are offered not for the truth of any particular statement made therein, but as circumstantial evidence of the Bureau's acknowledgement of the serious privacy implications of disclosing data at the census block level. Finally, official government statistics and publications are the kinds of documents upon which responsible people rely, and are thus properly considered by the Commission. *People v. ConAgra Grocery Prods. Co*., 17 Cal. App. 5th 51, 138 (2017) ("…if the documents that are being proffered are the product of a public agency, they will be admitted as an exception to the hearsay rule under Evidence Code Section 1280. That's a general proposition I don't think anyone can argue with.").

Moreover, although the official congressional testimony of the Director of the Federal Trade Commission's Bureau of Consumer Protection is technically hearsay, the testimony of a high ranking government official under oath and penalty of prosecution for lying to Congress

---

[114] D.22-05-003, p. 83

[115] See Fed. Rule of Evid. 803(8) (public records); 803(17) (compilations or publications relied upon by people in certain occupations); Ca. Evid. Rule 1280 (record by public employee); Ca. Evid. Rule 1340 (published compilation relied upon as accurate by business); See *Gilbrook v. City of Westminster*, 177 F.3d 839, 858 (9th Cir. 1999) (A trial court is entitled to presume that a public report is authentic and trustworthy.)

constitutes an admissible public record. *Nelson v. Gaunt*, 125 Cal. App. 3d 623 (1981) (admitting testimony of a public health official concerning dangers of silicone in malpractice suit concerning silicone breast implants). Even if it were not, it is certainly the kind of evidence upon which responsible persons would rely and is therefore admissible under Commission precedent.

Similarly, although the academic studies cited by Lyft, such as the published research report by MIT data scientists, are hearsay, the reports were prepared by leading scientists whose methods and assumptions are documented therein, and whose accuracy and reliability can be fairly evaluated by the Commission and accorded the weight appropriate thereto. This is significant because the reason administrative agencies are allowed to rely upon hearsay is that they are presumed to be more sophisticated than juries and can assess the appropriate weight to be accorded such evidence. *The Utility Reform Network v. Public Utilities Com.* (2014) 223 Cal.App.4th 945, 959–960 ("Administrative agencies like the Commission are given more latitude to consider hearsay testimony than are courts (ibid.), in part because 'factfinders in administrative proceedings are more sophisticated than a lay jury.'"); *Re Landmark Communications, Inc.* (1999) 84 C.P.U.C.2d 698, 701 (Commission can weigh hearsay evidence along with all other evidence); *cf. People v. Veamatahau* (2020) 9 Cal.5th 16, 29 ("As these examples make clear, an expert may consult specific sources in a case — a textbook, a treatise, or an academic paper — and supply the information found therein to the jury as background information without running afoul of the hearsay rules."); *People v. Bui* (2001) 86 Cal.App.4th 1187, 1196 ("Logan relied on scientific literature, statistical data, and an epidemiological study, all of which are the type of matter that reasonably may be relied on by an expert in forming an opinion."). Thus, the Commission may not, consistent with its own rules and longstanding precedent, use the hearsay rule as a way to avoid addressing evidence that is contrary to its desired outcome. It must determine whether the evidence is supported for the truth of the matter asserted or for a non-hearsay purpose, and if it is indeed hearsay, whether it falls within an exception or is the kind of evidence upon which responsible persons might rely. *See, e.g, Gregory v. State Bd. of Control* (1999) 73 Cal.App.4th 584, 596, *as modified on denial of reh'g* (July 27, 1999) ("Hearsay is admissible in an administrative hearing if it is relevant and 'the sort of evidence on which responsible persons are accustomed to rely in the conduct of serious affairs.'"). Only after so doing can the Commission assess the appropriate weight to be accorded to such evidence.

D.22-05-003 attempted to justify its refusal to consider Lyft's evidence by stating:

> The problem that Lyft is facing is one of authentication of the various studies and publications that its declarant did not author and does not have personal knowledge of the truth of their contents. Had Lyft obtained declarations from the authors of these studies, it would have overcome the hearsay evidentiary threshold and the Commission could have considered this evidence.

D.22-05-003, p. 117. But this attempted explanation conflates authentication and hearsay and only further muddies the waters. Authentication and hearsay are distinct and largely unrelated legal principles. *People v. Dawkins* (2014) 230 Cal.App.4th 991, 1004 ("the issues of hearsay and authentication are independent of one another."), *as modified* (Oct. 21, 2014). Authentication is any evidence sufficient to establish that "the writing is actually what its proponent claims it to be." *Osborne v. Todd Farm Service* (2016) 247 Cal.App.4th 43, 53; Evid. Code § 1401. As the court in *People v. Valdez* (2011) 201 Cal.App.4th 1429, 1435 explained, "[t]he author's testimony is not required to authenticate a document (§ 1411); instead, its authenticity may be established by the contents of the writing (§ 1421) or by other means." Thus, it is clearly not the case that Lyft must produce a declaration from the author of a document to authenticate it. Rosenthal's testimony is competent evidence that the documents are, in fact, what Lyft claims they are, and no one has questioned their authenticity. Nor would a declaration from the author of these articles solve any hearsay problem, as a declaration is a classic form of hearsay. *Rushing*, 2020 WL 2404666, at *33, citing *In re Fields*, 51 Cal. 3d 1063, 1070 (1990) ("[A]n out-of-court declaration is hearsay, and unless subject to some exception permitting it to be admitted, should be excluded upon timely and proper objection."); *Fortune,* 61 So.3d 441, 445 ("The affidavit, an out-of-court statement offered to prove the truth of the matter asserted, is the most basic form of hearsay."). As explained above, the evidence submitted by Lyft here is in most instances not hearsay at all, but in those instances which do qualify as hearsay, is the kind of evidence upon which responsible persons rely and is therefore admissible under the Commission's own rules and precedent.

Lastly, in this motion, Lyft seeks official notice of various items of evidence pursuant to Evidence Code § 452(c) and (h), as appropriate. *See* footnotes 78, 80, 94, 95, 97, and 99, *infra*. Pursuant to Rule of Practice and Procedure 13.10, "official notice may be taken of such matters as may be judicially noticed by the courts of the State of California pursuant to Evidence Code section 450 *et seq.*" Thus, the Commission can and should take official notice of such evidence and accord it the weight it deserves in consideration of its source, reasoning, and method of analysis.

IV. CONCLUSION

The Commission should follow longstanding precedent holding that regulated entities do not lose the right to protect their data by virtue of being regulated. Lyft has amply satisfied the requirements of the CUTSA to establish that the Census Block Trip Data qualifies as a trade secret. In addition, a determination that preservation of Lyft's trade secrets would work an injustice would be unsupported by substantial evidence and contrary to law.

Lyft has also amply demonstrated that disclosure of such data would present serious privacy concerns for the millions of Californians who regularly use TNCs. Exposing such a rich and comprehensive data set to public scrutiny can be reasonably anticipated to expose intimate private details of Californians who use TNCs and to expose them to danger, embarrassment, ridicule, or other harm from the exposure of their movements and activities. The Commission should grant Lyft's request for confidential treatment of the Trip Data.

Dated: June 21, 2022 **Lyft, Inc.**	**BRYAN CAVE LEIGHTON PAISNER LLP**	
By: */s/*Janeé C. Weaver */* _____	By:	*/s/Daniel Rockey/*
Janeé C. Weaver		Daniel Rockey
(415) 475-8459 janeeweaver@lyft.com	Attorneys for Lyft, Inc. (415) 268-1986 Daniel.Rockey@bclplaw.com	