FILED
11/24/21
02:04 PM

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

ADMINISTRATIVE LAW JUDGE'S 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

This *Ruling* grants, in part, the Motions of Uber Technologies, Inc., Lyft, Inc., HopSkipDrive, Inc., and Nomad Transit, LLC (sometimes referred to collectively as Moving Parties) for confidential treatment of portions of their 2021 Annual Transportation Network Company Reports. The *Ruling* finds that Moving Parties may redact the following information from the public versions of the 2021 Annual Reports on the grounds that the information is confidential:

- Latitude and longitude information in all data categories.
- Driver information in all data categories: drivers' names, type of driver identification, license state of issuance, license number, expiration date, description of allegation, definition, type and description of alleged sexual assault or sexual harassment, and vehicle VIN.
- Accidents and incidents: the parties involved in the incident, any party found liable in an arbitration proceeding, information concerning any criminal proceeding if the record has been sealed by the court,

> amounts paid by the TNC's insurance, driver's insurance, or by any other source.

The *Ruling* denies the balance of Moving Parties' Motions because they have failed to meet their burden of proving that the information is protected from disclosure on either trade secret or privacy grounds. Attachment A to this *Ruling* provides a category-by-category identification, which tracks the reporting template, of what information required by the 2021 Annual Report is confidential and what information should be made public.

This *Ruling* also will apply to *Motions for Confidential Treatment* that Nomad Transit, LLC and HopSkipDrive, Inc. filed for their 2020 Annual Reports.

1. Background

In accordance with Decision (D.) 20-03-014, Uber Technologies, Inc. (Uber), Lyft, Inc. (Lyft), HopSkipDrive, Inc. (HopSkipDrive), and Nomad Transit, LLC (Nomad) (sometimes referred to collectively as the Moving Parties) filed their respective motions for confidential treatment of information they categorize in different ways as trip data in their 2021 Annual Reports (Uber, Lyft, HopSkipDrive, and Nomad are sometimes referred to collectively as Moving Parties). Nomad and HopSkipDrive also ask that the confidentiality determinations made for Uber and Lyft's 2020 Annual Reports apply equally to the Nomad and HopSkipDrive 2020 Annual Reports.[1]

The resolution of Moving Parties' Motions requires a determination of whether trip data is trade secret and/or privacy protected. Trip data is not a universally defined term but, instead, refers to various data sets that the Commission has specified as being part of the Annual Report information requirements. Thus, although each Motion seeks to protect against the

[1] Nomad *Motion*, at 5; HopSkipDrive *Motion*, at 6.

disclosure of trip data categories, it will be helpful to identify the data fields required in the 2021 Annual Reports that Moving Parties argue should be redacted from the public versions because of trade secret, privacy, and/or public interest grounds so that the similarities between Moving Parties' Motions can be understood.

Uber argues that the following information is confidential: (1) trip data, including precise information such as pickup and drop-off locations; (2) driver information, including driver names and driver's license numbers; and (3) certain records of complaints, including reports made to Uber by riders and drivers, particularly in instances of sexual harassment or assault, and the disposition of those reports. (Uber *Motion*, at 4, and *passim*.) As legal support, Uber claims that the information is protected by Government Code § 6254(c)'s exemption for "files the disclosure of which would constitute an unwarranted invasion of personal privacy"; Government Code § 6254(k)'s exemption for "records, the disclosure of which is exempted or prohibited pursuant to federal or state law," which would by extension cover the California Uniform Trade Secrets Act which is codified at Civil Code §§ 3246 *et seq*; and Government Code § 6254.7(d), which provides that trade secrets are not public records under the California Public Records Act. (*Id*.)

Lyft argues the following information, which it refers to collectively as census block trip data, is confidential: (1) requests accepted; (2) requests accepted periods: (3) requests not accepted; and (4) assaults and harassments. (Lyft *Motion*, at 7-8, and *passim*.) Lyft makes legal arguments similar to Uber's, and also suggests that administrative law demands for data of private companies may "likely" violate a company's 4th Amendment rights. (*Id*., at 10.)

Nomad argues that the following information is confidential: (1) accidents and incidents report; (2) assaults and harassments report; (3) driver number of hours report; (4) driver number of miles report; (5) law enforcement citations report; (6) off platform solicitations report; (7) ride requests accepted report; (8) ride requests accepted period report; (9) ride requests not accepted report; (10) suspended drivers report; and (11) zero tolerance report. (Nomad *Motion*, Exhibit B thereto.) Nomad cites to the same statutory authorities in Uber's *Motion*. Nomad also cites to the public interest balancing test set forth in Government Code § 6255(a) which provides that information may be exempted from disclosure even if the information does not qualify for an exemption under any other section of the California Public Records Act where the public interest that is served by "not disclosing the record clearly outweighs the public interest served by disclosing the record." (Nomad *Motion*, at 14-15.)

HopSkipDrive argues that the following information is confidential: (1) Driver names and IDs report; (2) accidents and incidents report; (3) assaults and harassment report; (4) accessibility complaints report; (5) law enforcement citations report; (6) off platform solicitation report; (7) suspended drivers report; (8) zero tolerance report; (9) number of hours report; (10) number of miles report; (11) ride requests accepted report; (12) ride requests not accepted report; (13) rides requests accepted aggregate report and rides requests not accepted aggregate report; and (14) new report: ride requests accepted periods report. (HopSkipDrive *Motion*, 10-13.) HopSkipDrive cites to the same statutory authorities in Uber's *Motion* and the balancing test cited in Nomad's *Motion*. Since it is engaged primarily with the transport of minors, HopSkipDrive also claims confidentiality of certain information based on the Family Educational Rights and Privacy Act.

Moving Parties reference the 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 Confidentiality Ruling*), which resolved the trade secret and privacy arguments for certain data fields, and found that the following data fields were confidential on privacy grounds:

- Latitude and longitude information in all data categories.
- Driver information in all data categories: drivers' names, type of driver identification, license state of issuance, license number, expiration date, description of allegation, definition, type, and description of alleged sexual assault and sexual harassment, and vehicle VIN.
- Accidents and incidents: the parties involved in the incident, any party found liable in an arbitration proceeding, information concerning any criminal proceeding if the record has been sealed by the court, amounts paid by the TNC's insurance, driver's insurance, or by any other source.

Where the *2020 Confidentiality Ruling* found certain data fields to the 2020 Annual Reports to be confidential on privacy grounds, some Moving Parties ask that those same findings apply to the same categories for the 2021 Annual Reports. (*See* Lyft *Motion*, at 2-6; HopSkipDrive *Motion*, at 3-5; Nomad *Motion*, at 5-6.)

This *Ruling* agrees with Moving Parties' request but with one exception: information required by waybills. Upon further reflection, this *Ruling* finds that waybill information is not protected on privacy grounds and is not entitled to trade secret protection. Waybill numbers in the data dictionary refer to Waybill 1, Waybill 2, Waybill 3 and up to Waybill 7. These 7 separate Waybill numbers are separate columns and are there in case there is a shared ride. In a shared ride, there is a separate waybill number which refers to a specific

passenger's trip. For example, if a shared ride has two passengers, then Waybill 1 will refer to the Waybill number for Passenger 1 and Waybill 2 will refer to the Waybill number for Passenger 2 in a trip. As these numbers do not reveal personal information about a passenger, they are not protected from public disclosure on privacy grounds.

As to the balance of the trip data fields required for the 2021 Annual Reports that the *2020 Confidentiality Ruling* determined was neither trade secret nor privacy protected, Moving Parties renew their previously rejected arguments but have supplemented both their evidentiary showing and legal authority to support their confidentiality claims. Since these motions seek to shield from public disclosure a great deal of information about trips that TNCs provide to California passengers, it will be necessary to set forth the applicable law for establishing and resolving claims for confidential treatment (on trade secret grounds, privacy grounds, or both), particularly in light of California's public policy favoring the disclosure of information in the government's possession in order to promote transparency in the government's regulatory activities.

2. Applicable Laws Regarding Confidential Treatment of Information Provided to the Commission

D.20-03-014 requires that any claim for confidential treatment of information provided to the Commission must be justified with particularized references to the type of information sought to be shielded from public disclosure, the law that supports the claim of confidentiality, and a declaration under penalty of perjury that sets forth the factual justification with the requisite granularity.[2] Placing the burden on the TNC to substantiate its claim of

[2] D.20-03-014, Ordering Paragraph 2.

confidentiality is consistent with the general rule regarding allocating the burden of proof. Pursuant to Evidence Code § 500: "except as otherwise provided by law, a party has the burden of proof as to each fact essential to its claim or defense." (*See also Aguilar v. Atlantic Richfield Co*. (2001) 25 Cal.4th 826, 861; *Samuels v. Mix* (1999) 22 Cal.4th 1, 10-11; and *Bridgestone/Firestone, Inc. v. Superior Court* (1992) 7 Cal.App.4th 1384, 1393, *hearing denied, and opinion modified* [party claiming privilege has burden of proving that information qualifies as a protected trade secret].)

In addition, D.20-03-014's strict evidentiary showing to substantiate a claim of confidentiality is derived from and reflects California's strong public policy favoring access to government records. The California Constitution's mandate provides that the public has the right to access most Commission records. Cal. Const. Article I, § 3(b)(1) states:

> The people have the right of access to information concerning the conduct of the people's business, and, therefore, the meetings of public bodies and the writings of public officials and agencies shall be open to public scrutiny.[3]

The California Public Records Act (CPRA) requires that public agency records be open to public inspection unless they are exempt from disclosure under the provisions of the CPRA.[4] The Legislature has declared that "access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state."[5]

---

[3] *See e.g., International Federation of Professional & Technical Engineers, Local 21, AFL-CIO v. Superior Court* (2007) 42 Cal.4th 319, 328-329.

[4] *See Roberts v. City of Palmdale* (1993) 5 Cal.4th 363, 370. ("The Public Records Act, Section 6250 *et seq*., was enacted in 1968 and provides that "every person has a right to inspect any public record, except as hereafter provided." (§ 6253, subd. (a).)

[5] Government Code § 6250.

The CPRA requires the Commission to adopt written guidelines for access to agency records, and requires that such regulations and guidelines be consistent with the CPRA and reflect the intention of the Legislature to make agency records accessible to the public.[6] General Order (GO) 66-D, effective January 1, 2018, constitutes the Commission's current guidelines for access to its records, and reflects the intention to make Commission records more accessible.[7] GO 66-D also sets forth the requirements that a person must comply with in requesting confidential treatment of information submitted to the Commission. D.20-03-014 made clear that a person submitting information to the Commission must satisfy the requirements of GO 66-D to substantiate a claim for confidentiality treatment of information.[8]

This *Ruling* applies the forgoing legal standards to Moving Parties' claims for confidential treatment for certain information contained in their 2021 Annual Reports.

3. Compliance with the 2021 Annual Reports Does Not Trigger Fourth and Fifth Amendment Considerations.

3.1. The Commission's Regulatory Power to Require a TNC to Disclose Non-Private Trip Data Does Not Amount to An Unreasonable Search and Seizure under the Fourth Amendment

This *Ruling* has set forth both the foregoing policy favoring public disclosure, as well as the high burden that a party must demonstrate to prevent such a disclosure, in order to place Lyft's argument regarding the right to protect TNC data against unreasonable searches and seizures in the proper legal

[6] Government Code § 6253.4(b).

[7] *See* D.17-09-023 at 11-12, 14.

[8] D.20-03-014 at 23.

context.[9] (Lyft *Motion*, at 9-12.) Lyft cites *Patel v. City of Los Angeles*, (9th Cir. 2013) 738 F.3d 1058, 1061-1062, and 1064, *aff'd sub nom. City of Los Angeles, Calif. v. Patel* (2015) 135 S.Ct. 2443 (2015), for the proposition that the government may require businesses to maintain records containing private information covered by the Fourth Amendment to the U.S. Constitution and to make that information available for routine inspection when necessary to further a legitimate regulatory interest.[10] This *Ruling* has no quarrel with that legal proposition but notes two important distinctions that make it inapplicable to Lyft's *Motion*: first, the parties in *Patel* did not dispute whether the information at issue was private. In contrast, the trip data information in dispute has no presumption of privacy and, as this *Ruling* will demonstrate, is not private. Second, *Patel* dealt with the government's ability to collect seemingly private data. In contrast, Lyft is not contesting the Commission's ability to require Lyft to collect and report data that Lyft claims is private. Instead, the question this *Ruling* must resolve is whether the trip data that Lyft has provided to the Commission in the Annual Reports may be disclosed to the public.

Lyft's argument that having to publicly disclose trip data implicates Fourth Amendment considerations is not supported by its reliance on two recent decisions involving Airbnb. Lyft cites *Airbnb, Inc. v. City of New York* (*Airbnb New York)*[11] and *Airbnb, Inc. v. City of Boston (Airbnb Boston)*[12] as proof that administrative demands for data of private companies likely violated Airbnb's

[9] *Motion*, at 9-12.

[10] *Id.*, at 9-10.

[11] (S.D.N.Y. 2019 373 F.Supp.3d 467, 484, *appeal withdrawn*, No. 19-288, 2019.

[12] (D. Mass. 2019) 386 F.Supp.3d 113, 125, *appeal dismissed* (1st Cir., Sept. 3, 2019).

Fourth Amendment rights.[13] Lyft quotes the following two passages from *Airbnb New York*:

> [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 user-related records that "are more than sufficient to trigger Fourth Amendment protection. …
>
> 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 competingplatforms 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.[14]

But to understand the impetus why the Court was concerned about the potential breach of privacy rights, it will be helpful to examine the ordinance that Airbnb challenged. In an effort to crack down on short-term rentals that violated New York's Multiple Dwelling Laws, the New York City Council approved an ordinance that applied to booking services offered by online, computer, or application-based platforms. Each booking service was required to submit a

[13] *Motion*, at 10.

[14] *Id.*, at 10-11.

monthly transaction report that must include for every short-term rental listed on the platform: the physical address of the short-term rental associated with each transaction, including the street name, street number, apartment or unit number, borough or county, and zip code; the full legal name, physical address, phone number and email address of the host of such short term rental; the individualized name and number and the URL of such advertisement or listing; the number of days the unit was on the platform; and the fees received.[15] Asking for actual names and addresses of the rental property and the host is similar to the type of information that the United States Supreme Court has recognized as private and that the infringement by the government into that area of privacy can trigger Fourth Amendment concerns. (*See Katz v. United States* (1967) 389 U.S. 347, 360-361; *Oklahoma Press Pub. Co. v. Walling* (1946) 327 U.S. 186, 202 [Court held that the Fourth Amendment applied to administrative subpoenas *duces tecum* issued in an investigation into violations of the Fair Labor Standards Act].)

In contrast with the private information that New York and Boston were requiring the rental platform companies to provide, Lyft is under no similar danger that such private information will be publicly disclosed. California law recognized that personally identifiable information that is obtained by a government agency like the Commission is generally protected against public

[15] *Airbnb New York, supra*, 373 F.Supp.3d at 474. The ordinance at issue in *Airbnb Boston* contained similar reporting requirements. (386 F.Supp.3d at 118): "A Booking Agent shall provide to the City, on a monthly basis, an electronic report, in a format determined by the City, ... of the listings maintained, authorized, facilitated or advertised by the Booking Agent within the City of Boston for the applicable reporting period. The report shall include a breakdown of where the listings are located, whether the listing is for a room or a whole unit[.]"

disclosure.[16] The *2020 Confidentiality Ruling* agreed with Uber and Lyft that such personally identifiable information could be redacted from the public version of the TNC Annual Reports.[17] The *2020 Confidentiality Ruling* also agreed that latitude and longitude information could also be redacted from the public version of the TNC Annual Reports since this information could be used to deduce an actual starting and ending address for a TNC passenger trip.

But the balance of the trip data, (such as zip code and census block information, as well as the rest of the categories identified in Attachment A to this *Ruling*) does not implicate such constitutionally recognized privacy protections so the right to be protected from actions that possibly violate the Fourth Amendment is not implicated. The Commission addressed its regulatory power to compel TNCs to provide trip data in the Annual Reports in D.16-01-014. Rasier-Ca, LLC, Uber's wholly owned subsidiary, challenged, on Fourth Amendment privacy grounds, the Commission authority to require TNCs to submit Annual Reports. The Commission's reasoning is instructive and bears repeating here. The Commission determined that its power to regulate TNCs and to require TNCs to submit Annual Reports was analogous to *California Bankers Association v. Shultz* (1974) 416 U.S. 21, 66-67, wherein the Supreme Court held that the Secretary of State's requirement that banks file reports dealing with particular phases of their activities did not violate the Fourth Amendment. The banks were not mere strangers or bystanders with respect to the transactions that

[16] (*See*, *e.g.*, Government Code § 6254(c) [personnel, medical or similar files]; and Government Code § 6254.16 [utility customer information unless disclosure is authorized by recognized exception].)

[17] *See 2020 Confidentiality Ruling*, at 8 ("Moving Parties argue that the driver's personal information [*i.e.* driver's first and last name, middle initial, type of identification, the driver's driver license state of issuance, number, expiration date, and VIN of the vehicle] should be treated as confidential. This *Ruling* agrees with that request.")

they were required to report. To the contrary, the banks were parties to the transactions and earn portions of their income from conducting such transactions and may have kept reports of these transactions for their own purposes. Similarly, the TNCs such as Lyft are in the business of making transportation services available to customers and are undoubtedly keeping trip data information on these rides. Thus, Fourth Amendment protections against government searches and seizures are not triggered.

This *Ruling* notes that TNCs have had their Fourth Amendment challenges rejected in other jurisdictions and have been required to produce trip data. In *Carniol v. New York City Taxi & Limousine Comm'n* (Sup. Ct. 2013) 975 N.Y.S.2d 842, the Court rejected Uber's challenges to providing trip data because the expectation of privacy was not present. In reaching its decision, the Court cited to *Minnesota v. Carter* (1998) 525 U.S. 83, 88 in which the United States Supreme Court stated that a party may not prevail on a Fourth Amendment claim unless the party can show that the search and seizure by the state infringed on a legitimate expectation of privacy. Where a government entity is vested with broad authority to promulgate and implement a regulatory program for the regulated transportation industry, those participating "have a diminished expectation of privacy, particularly in information related to the goals of the industry regulation." (*Buliga v. New York City Taxi Limousine Comm'n* (2007) WL 4547738 *2, *affd sub nom. Buliga v. New York City Taxi & Limousine Comm'n* 324 Fed Appx 82 (2d Cir. 2009); and *Statharos v. New York City Taxi & Limousine Comm'n* (2d Cir. 1999) 198 F.3d 317, 325.) This is true even beyond the transportation industry since the key consideration is whether the industry is closely regulated. The United States Supreme Court recognized that the greater the regulation the more those subject to the regulation can expect intrusions

upon their privacy as it pertains to their work. (*Vernonia Sch. Dist. 47J v. Acton* (1995) 515 U.S. 646, 657.)

TNCs in California also have a diminished expectation of privacy with respect to providing trip data in their Annual Reports in light of the Commission's extensive jurisdiction over TNCs. As provided in Article XII of the California Constitution and the Charter-party Carriers' Act (Pub. Util. Code § 5351 *et seq.*), the Commission has for decades been vested with a broad grant of authority to regulate TCPs. For example, Pub. Util. Code § 5381 states:

> To the extent that such is not inconsistent with the provisions of this chapter, the commission may supervise and regulate every charter-party carrier of passengers in the State and may do all things, whether specifically designated in this part, or in addition thereto, which are necessary and convenient in the exercise of such power and jurisdiction.

This Commission found in D.13-09-045 that TNCs were TCPs subject to the Commission's existing jurisdiction.[18] Pursuant to GO 157-D, Section 3.01, providers of prearranged transportation are required to maintain waybills which must include, at a minimum, points of origination and destination. Pursuant to GO 157-D, Section 6.01, every TCP is required to maintain a set of records which reflect information as to the services performed, including the waybills described in Section 3.01. The Commission also found that it would expand on its regulations regarding TCPs and utilize its broad powers under Pub. Util. Code § 701 to develop new categories of regulation when a new technology is introduced into an existing industry.[19] Given this expansive authority, TNCs would certainly have reason to expect intrusions upon their alleged privacy as it

[18] D.13-09-045, at 23.

[19] *Id*.

relates to the provision of TNC services. Accordingly, Lyft's Fourth Amendment claims are inapplicable.

But even if the Fourth Amendment was implicated, the Commission established in D.13-09-045 its legitimate regulatory interest in requiring every regulated TNC to submit an Annual Report that is populated with the information required by the Commission's template. What *Patel* did not address, and what this *Ruling* does address, is whether a party has met its burden of proving that certain information that must be submitted as part of the Annual Report is exempt from public disclosure. As such, the facts and issue before the Commission are distinguishable from *Patel*, *Airbnb New York*, and *Airbnb Boston*. Unlike the positions New York and Boston advocated in those two decisions, the Commission is not stating that Lyft or any other TNC lacks the right to assert an expectation of privacy regarding TNC data collected and reported at the Commission's behest. Instead, what the Commission held since it ended the presumption of confidentiality for TNC Annual Reports is that the TNC asserting a claim of confidentiality or other privilege must establish that claim with the requisite granularity.

3.2. Since the Commission is Not Requiring the Public Disclosure of Protected Trip Data, Lyft Fails to Establish an Unlawful Misappropriation to Trigger a fifth Amendment Regulatory Takings Argument

Lyft asserts that the law protects the trade secrets of private companies from forcible disclosure by regulatory agencies, and cites *Bridgestone/Firestone, supra,* 7 Cal.App.4th 1384, 1391, for the rule that disclosure may be compelled where to do otherwise would tend to conceal fraud or work a serious injustice.[20]

[20] *Motion*, at 12.

Lyft goes further and claims that a government agency's use of private, investment-backed trip data submitted by a regulated entity may constitute an unlawful misappropriation or taking in violation of the Fifth Amendment to the Constitution.[21]

Initially, this *Ruling* questions how seriously Lyft is making its regulatory takings argument. First, Lyft uses the words "may constitute an unlawful Taking under the Fifth Amendment[,]" rather than an unlawful taking has or will occurred. Second, Lyft uses the phrase "may constitute unlawful misappropriation" in violation of the California Uniform Trade Secrets Act (CUTSA) without setting forth the elements of a misappropriation claim. In *Syngenta Crop Protection, Inc. v. Helliker* (2006) 138 Cal.App.4th 1135, 1172, a case which Lyft cites in its *Motion*, the Court set forth the elements for a misappropriation cause of action:

> "Misappropriation" is defined to include "use of a trade secret of another without express or implied consent by a person who: [¶] . . . [¶] [a]t the time of . . . use, knew or had reason to know that his or her knowledge of the trade secret was: [¶] . . . [¶] [a]cquired under circumstances giving rise to a duty to maintain its secrecy or limit its use." (Civ. Code, § 3426.1, subd. (b).)

Absent from Lyft's *Motion* is any suggestion that the Commission was under a duty to maintain the alleged secrecy of the trip data or limit its use. In *Ruckelshaus v. Monsanto Co.* (1984) 467 U.S. 986, 1008, which Lyft also relies upon in its *Motion*, the Supreme Court explained that the duty to maintain the secrecy of trade secret information could be established by demonstrating that the government entity receiving the information provided a "guarantee of

[21] *Id.*

confidentiality or an express promise." The Supreme Court's discussion on this point is instructive as it underscores the failure on Lyft's part to fully develop its regulatory takings claim:

> But the Trade Secrets Act is not a guarantee of confidentiality to submitters of data, and, absent an express promise, Monsanto had no reasonable, investment-backed expectation that its information would remain inviolate in the hands of EPA. In an industry that long has been the focus of great public concern and significant government regulation, the possibility was substantial that the Federal Government, which had thus far taken no position on disclosure of health, safety, and environmental data concerning pesticides, upon focusing on the issue, would find disclosure to be in the public interest. Thus, with respect to data submitted to EPA in connection with an application for registration prior to October 22, 1972, the Trade Secrets Act provided no basis for a reasonable investment-backed expectation that data submitted to EPA would remain confidential.

Similarly, Lyft fails to point to any guarantee of confidentiality or an express promise that trip data would be exempted from public disclosure on privacy (*i.e.,* trade secrets) grounds. In fact, with the elimination of the presumption of confidentiality in 2020 by the adoption of D.20-03-014, Lyft knew that the only way it could prevent the public disclosure of any part of its 2020 Annual Report was to file a motion complete with a declaration that detailed each claim for confidentiality, which it did and which the Administrative Law Judge (ALJ) rejected, in part, in his *2020 Confidentiality Ruling* as being factually insufficient.

Lyft's other authorities are even more attenuated as they do not address the right and duty to publicly disclose TCP or TNC information. At best, the

authorities cited on pages 12 and 13 of Lyft's *Motion*[22] deal with categories of information that the Commission has recognized as confidential following a sufficient factual or legal showing.[23] Nor is Lyft's position buttressed by the cite to the Commission's recent D.20-12-021,[24] in which the Commission ordered the Network Study to be disclosed to the public except for those portions that might pose a security risk, the Commission acknowledged that "there are times to be concerned about full public disclosure of proprietary data. Classic examples are customer lists, true trade secrets, and prospective marketing strategies where there is full blown—and not peripheral—competition."[25] In none of these

---

[22] Lyft cites *Application of Pac. Gas & Elec. Co. (U39E) for Comm'n Approval Under Pub. Utilities Code Section 851 of an Irrevocable License for Use of Util. Support Structures & Equip. Sites to Extenet Sys. (California) LLC.* (Oct. 27, 2016) 2016 WL 6649336, at *3; *Order Instituting Rulemaking on Com'n Own Motion into Competition for Local Exch. Serv.* (Oct. 22, 1998) 82 CPUC 2d 510, at *36 ("Parties providing confidential information should be permitted to redact nonessential data and require that nondisclosure agreements be signed by those individuals who are provided access to such materials."); *Order Instituting Rulemaking on Commission's Own Motion into Competition for Local Exch. Serv.* (Sept. 2, 1999) 1999 WL 1112286, at *1 (sealing "proprietary business information concerning Ameritech's proposed operations for its first and fifth year of operations"); *In Re S. California Edison Co.*, No. 04-12-007, 2005 WL 1958415, at *1 (Aug. 9, 2005) (granting confidential treatment for number of bids received, total capacity offered to utilities from wind projects, and average price of bids, and accepting representation that "disclosure of the redacted information could drive up the price of contracts in RPS solicitations [and] reduce competition by leading certain bidders to refrain from participating in the RPS process").

[23] Lyft cites *Application of San Diego Gas & Elec. Co. (U902e) for Approval of Its 2018 Energy Storage Procurement & Inv. Plan. & Related Matter*, No. 18-02-016, 2019 WL 3017166 (June 27, 2019) at *50 (confidential versions of prepared testimony that "contain cost information related to scoring and evaluating bids in competitive solicitations … is entitled to confidential treatment"); *Application of S. California Edison Co. (U338e) for Approval of Its Forecast 2019 Erra Proceeding Revenue Requirement*, No. 18-05-003, 2019 WL 1204904 (Feb. 21, 2019) at *22 (the Commission confirmed that it "is interested in ensuring that the public has access to information related to utility rates, but also has its own rules to protect the confidentiality of market sensitive information").

[24] *Decision Addressing Carriers' Confidentiality Claims Related to Network Study Ordered in Decision 13-02-023, as Affirmed in Decision 15-08-041.*

[25] *Motion*, at 13.

decisions, however, did the Commission say that its determinations of confidentiality or recognition of certain market sensitive data would have the universal application that Lyft seems to suggest. Lyft cannot point to any Commission law that, since 2020, has granted such blanket protection to TNC trip data.[26]

But even if Lyft could overcome the foregoing hurdles, its Fifth Amendment challenge would still fail because the Commission's regulatory actions would not give rise to a regulatory-takings claim. As noted above, the Takings Clause, which is deemed applicable to the states *via* the Fourteenth Amendment,[27] is found in the Fifth Amendment of the U.S. Constitution and provides that "nor shall private property be taken for public use, without just compensation." The purpose behind the clause is "to bar Government from forcing some people alone to bear public burdens which, in all fairness and justice, should be borne by the public as a whole." (*Armstrong v. United States* (1960) 364 U.S. 40, 49.) While takings law had its genesis in real property disputes, over time the United States Supreme Court expanded the constitutional protection of property beyond the concepts of title and possession and sought to protect the value of investments against governmental use or regulation. (*See Pennsylvania Coal Co. v. Mahon* (1922) 260 U.S. 393, 415 ["while property may be regulated to a certain extent, if regulation goes too far it will be

[26] Moreover, D.20-12-021, at 17, also pointed out that even if a trade secret claim has been established, the Commission must determine if the assertion of such a privilege would tend to conceal fraud or otherwise work an injustice. As this *Ruling* will demonstrate, the "otherwise work an injustice" criterion is met here.

[27] *Palazzolo v. Rhode Island* (2001) 533 U.S. 606, 617 ("The Takings Clause of the Fifth Amendment, applicable to the States through the Fourteenth Amendment, *Chicago, B. & Q. R. Co.* v. *Chicago,* 166 U.S. 226, 41 L. Ed. 979, 17 S. Ct. 581 (1897), prohibits the government from taking private property for public use without just compensation.")

recognized as a taking."])[28] In *Lingle v. Chevron U.S.A., Inc.* (2005) 544 U.S. 528, 538, the United States Supreme Court recognized two categories of regulatory takings for Fifth Amendment purposes: first, where government requires an owner to suffer a permanent physical invasion of the property; and second, where the government regulation completely deprives an owner of all economically beneficial use of the property.[29]

These two categories of regulatory taking must be weighed against the deference that must be accorded to the decisional authority of state regulatory bodies. In *Duquesne Light Co. v. Barasch* (1989) 488 U.S. 299, 313-314, the Supreme Court discussed the deference that should be given to both state legislative bodies, as well as state public utilities commissions that are an extension of the legislature:

> It cannot seriously be contended that the Constitution prevents state legislatures from giving specific instructions to their utility commissions. We have never doubted that state legislatures are competent bodies to set utility rates. And the Pennsylvania PUC is essentially an administrative arm of the legislature [citations omitted.] We stated in *Permian Basin* that the commission "must be free, within the limitations imposed by pertinent constitutional and statutory commands, to devise methods of regulation capable of equitably reconciling diverse and conflicting interests."…

---

[28] California law also has a takings clause. Article I, Section 19 of the California Constitution provides in part: "Private property may be taken or damaged for public use only when just compensation, ascertained by a jury unless waived, has first been paid to, or into court for, the owner."

[29] *See also Lucas v. South Carolina Coastal Council* (1992) 505 U.S. 1003, 1027-1028, where the Supreme Court recognized that by reason of the State's traditionally high degree of control over commercial dealings, regulations can constitutionally render personal property economically worthless. To be an unconstitutional taking, the property right has to have been "extinguished." (*Ruckelhaus, supra,* 467 U.S. 986, 1002.)

As such, other courts have also recognized that "every statute promulgated by the Legislature is fortified with a strong presumption of regularity and constitutionality." (*Keystone Insurance Co. v. Foster*, 732 F. Supp. 36 (E.D. Pa. 1990); *Illinois v. Krull*, (1987) 480 U.S. 340, 351 (["Indeed, by according laws a presumption of constitutional validity, courts presume that legislatures act in a constitutional manner."] (*See e.g., McDonald* v. *Board of Election Comm'rs of Chicago* (1969) 394 U.S. 802, 809 ["Legislatures are presumed to have acted constitutionally even if source materials normally resorted to for ascertaining their grounds for action are otherwise silent, and their statutory classifications will be set aside only if no grounds can be conceived to justify them."])

The concern for respecting state legislative action is applicable to the Commission's regulatory activities. The Commission derives some of its powers from Article XII of the California Constitution and by powers granted from the Legislature. (*People v. Western Air Lines, Inc.*(1954) 42 Cal.2d, 621, 634 ["The Commission is therefore a regulatory body of constitutional origin, deriving certain of its powers by direct grant from the Constitution which created it. (*Pacific Tel. & Tel. Co.* v. *Eshleman* (1913), 166 Cal. 640 [137 P. 1119, Ann.Cas. 1915C 822, 50 L.R.A.N.S. 652]; *Morel* v. *Railroad Com*. (1938), 11 Cal.2d 488 [81 P.2d 144].) The Legislature is given plenary power to confer other powers upon the Commission. Art. XII, §§ 22 and 23.)"].)

In *Penn Central Transportation Co v. New York City* (1978) 438 U.S. 104, 124, the Supreme Court acknowledged that it has been unable to develop any set formula for determining when government action has gone beyond regulation and constitutes a taking. Nevertheless, *Penn Central* set forth several factors that have particular significance:

- The economic impact of the regulation on the claimant;
- The extent to which the regulation has interfered with distinct investment-backed expectations that the integrity of the trade secret will be maintained; and
- The character of the governmental action.

While written in the conjunctive rather than the disjunctive, some decisions suggest that a reviewing court "may dispose of a takings claim on the basis of one or two of these factors." (*Allegretti & Co. v. County of Imperial* (2006) 138 Cal.App.4th 1261, 1277; *Bronco Wine v. Jolly*(2005) 129 Cal. App.4th 988, 1035 ["The court may dispose of a takings claim on the basis of one or two of these factors. (*Maritrans Inc. v. United States* (Fed. Cir. 2003) 342 F.3d 1344, 1359 [where the nature of the governmental action and the economic impact of the regulation did not establish a taking, the court need not consider investment-backed expectations]; *Ruckelshaus v. Monsanto Co., supra*, 467 U.S. 986, 1009] [disposing of takings claim relating to trade secrets on absence of reasonable investment-backed expectations prior to the effective date of the 1972 amendments to the Federal Insecticide, Fungicide, and Rodenticide Act].) But for completeness's sake, and consistent with how rules are interpreted and applied when clauses are separated by a conjunctive, we will evaluate Lyft's takings argument against all of the criteria set forth, *supra*, in both *Lingle* and in *Penn Central*.

Lyft fails to establish that providing trip data meets either definition of a regulatory taking set forth in *Lingle*. First, there is no permanent physical invasion into Lyft's property. Instead, the trip data is information that the Commission has ordered all TNCs to maintain and report upon in the manner required by D.13-09-045. What is involved is the electronic transfer of information that will be analyzed and evaluated by the Commission as part of its regulatory responsibility over the TNC industry. Second, compliance with

Reporting Requirement j does not deprive Lyft of all economically beneficial use of its property. To the contrary, Lyft is free to continue analyzing trip data in order to refine or adjust its transportation business model for the TNC drivers and passengers who subscribe to the Lyft App.

Lyft's regulatory takings argument also fails under the *Penn Central* factors. With respect to the character-of-the-governmental-action prong, a takings claim is less likely to be found "when interference arises from some public program adjusting the benefits and burdens of economic life to promote the common good." (*Penn Central*, *supra*, 438 U.S. at 124.) Here, the reason for requiring the trip data in the manner prescribed is for the Commission to continue reviewing its regulations over the TNC industry in order to evaluate the impact on the riding public. Determining who is being served, what areas are being served, and the volume can assist the Commission in deciding if this new mode of transportation is being made available to all customers utilizing the Lyft app for service. Equal access to a regulated transportation service is the common good that is one of the prime goals of the Commission's regulatory authority over the transportation industry.

Lyft's argument also fails under the economic-impact prong. Here the inquiry is whether the regulation impairs the value or use of the property according to the owners' general use of their property. (*Phillip Morris v. Reilly* (2002) 312 F.3d 24, 41, citing *Pruneyard Shopping Center v. Robins* (1980) 447 U.S. 74, 83.) In contrast to *Phillip Morris*, where Massachusetts required tobacco companies to submit their lists of all ingredients used in manufacturing tobacco products so that this information could be disclosed to the public, the Commission has not ordered Lyft to submit the algorithms or other criteria utilized to market its service. It is just the resulting trip information that the

Commission requires and this *Ruling* is ordering be made publicly available. In sum, even if Lyft's trip data were a trade secret, neither the value of the property, nor the use to the property, has been impaired or extinguished simply by providing the information to the Commission or if the Commission orders the trip data at issue be publicly disclosed.

Finally, Lyft's argument fails under the investment-backed-privacy-expectation standard. As the Supreme Court explained in *Webb's Fabulous Pharmacies, Inc. v. Beckwith* (1980) 449 U.S. 155, 161, property interests, and the privacy expectations attendant thereto, "are not created by the Constitution. Rather, they are created and their dimensions are defined by existing rules or understandings that stem from an independent source such as state law." Here, there is no California law or controlling federal law holding that the trip data at issue is inherently private or that the creation of same invests it with some sense of privacy. Indeed, Lyft was aware that the Commission ordered all TNCs to create the Annual Reports so that the Commission could determine how its regulations were working and if any adjustments would be needed. In other words, Lyft's claim of a privacy expectation is subject to the Commission's power to regulate TNCs for the public good. Moreover, even if there was a distinct investment-backed expectation, "a taking through an exercise of the police power occurs only when the regulation 'has nearly the same effect as the complete destruction of [the property] rights' of the owner." (*Pace Resources, Inc. v. Shrewsbury Tp.* (3rd Cir. 1987) 808 F.2d 1023, 1033, quoting *Keystone Bituminous Coal Association v. Duncan* (3d Cir. 1985) 771 F.2d 707, 716, *aff'd* (1987) 480 U.S. 470.) There is no complete destruction of Lyft's property as it can utilize its trip data for whatever legitimate business purposes it deems appropriate.

In sum, Lyft fails to substantiate its unconstitutional regulatory takings argument.

4. Elements of a Trade Secret Claim

In 1984, California adopted, without significant change, the Uniform Trade Secrets ACT (UTSA). (Civil Code §§ 3426 through 3426.11. *DVD Copy Control Assn., Inc. v. Bunner (2003) 31 Cal. 4th 864, 874*; *Cadence Design Systems, Inc. v. Avant! Corp*. (2002) 29 Cal.4th 215, 221.) A trade secret has three basic elements:

- Information such as a formula, pattern, compilation, program, device, method, technique, or process;
- 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; and
- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Civil Code § 3426.1(d)'s three requirements are written in the conjunctive, rather than the disjunctive, meaning that all three requirements must be satisfied to successfully establish a trade secret claim. This approach is in accordance with decisions that have construed statutory provisions with the words "and" or "or' between the requirements. (*See Pueblo of Santa Ana v. Kelly* (D.N. Mexico 1996) 932 F.Supp. 1284, 1292 ["In this Section, the compact requirement is separated from the requirement that the compact be approved by the Secretary by the conjunctive term "and", indicating that Congress recognized as distinct the existence of a valid tribal-state compact and the approval of the Secretary putting that compact into effect."]; and *Azure v. Morton* (9th Cir. 1975) 514 F.2d 897, 900 ["As a general rule, the use of a disjunctive in a statute indicates alternatives and

requires that they be treated separately."].) Thus, the failure to satisfy any one of the three required elements dooms a trade secret protection claim.[30]

4.1. Moving Parties They Fail to Meet Their Burden of Proving that Trip Data is Trade Secret Protected

4.1.1. Trip Data is Not a Novel or Unique Compilation

Civil Code § 3426.1(d) refers to information and includes, as examples, formulas, patterns, compilations, programs, devices, methods, techniques, or processes. While it is true that the word "information" has a broad meaning,[31] trade secrets usually fall within one of the following two broader classifications: first, technical information (such as plans, designs, patterns, processes and formulas, techniques for manufacturing, negative information, and computer software); and second, business information (such as financial information, cost and pricing, manufacturing information, internal market analysis, customer lists, marketing and advertising plans, and personnel information). The common thread going through these varying types of information is that it is something that the party claiming a trade secret has created, on its own, to further its business interests.

---

[30] This *Ruling* does not address whether trip data that is compiled for dual purposes (*i.e.* pursuant to a government obligation and to further private business interests) can qualify as a trade secret in the first instance. Other jurisdictions have considered this question with respect to trip data and other data and have reached differing conclusions. (*See*, *e.g.*, *Spokane Research v. City of Spokane* (1999) 96 Wn. App.. 565, 578 ["It is illogical for the Developers to claim the studies were at the outset trade secrets in this context because the studies were produced for the City, not the Developers."]; and *Lyft, Inc., et al., v. City of Seattle* (2018) 190 Wn.2d 769 [The Washington Supreme Court acknowledged that it was "a close call" and that "while the evidence is mixed and the question is not beyond debate," it affirmed the superior court's conclusion that the zip code reports were trade secrets within the meaning of the UTSA.].)

[31] *Altavion, Inc. v. Konica Minolta Systems Laboratory, Inc*., *supra*, 226 Cal.App.4th, at 53.

This *Ruling* focuses on the word "compilation" from Civil Code § 3426.1 because it appears to be the most on point characterization of the trip data that Moving Parties assert is a trade secret. (*See* Declaration of Uttara Sivaram on Behalf of Uber Technologies, Inc. [Sivaram Decl., ¶ 3 [referring to the information required by the Commission as "a large dataset that includes information for every Uber trip in California[.]"]; Rosenthal Decl., ¶ 7 ["The data is continually *collected, compiled* and analyzed[.]"]; and Declaration of Saar Golde in Support of Nomad Transit LLC's Motion for Confidential Treatment [Golde Decl.], ¶ 2 ["I oversee the Data Science team, which is responsible for *collecting and reporting* aggregated and trip-level data to regulators[.]"]) While HopSkipDrive attempts to refer to trip data as "essentially a customer list," this *Ruling* rejects that analogy. (*See* Declaration of Trish Donahue on Behalf of HopSkipDrive [Donahue Decl.], ¶ 9.) The Commission has specified data categories regarding TNC passenger trips that must be populated with various details, not, as Ms. Donahue wrongly asserts by analogy, driver identifications. Without question, then, the trip data that Moving Parties must provide is a compilation.

Finding that trip data constitutes a compilation, however, does not end the Commission's inquiry into whether a compilation is entitled to trade secret protection. For a compilation to be a trade secret the information has to be grouped in a unique valuable way, even though the discrete elements that make up the compilation would not qualify as a separate trade secret. Otherwise, any compilation of information could arguably be considered a trade secret.

The requirement that Moving Parties must demonstrate that the compilation of trip data is novel or unique finds support in California law. (*See Morlife, Inc. v. Perry* (1997) 56 Cal.App.4th 1514, 1523 [Customer list was a unique "compilation, developed over a period of years, of names, addresses, and

contact persons, containing pricing information and knowledge about particular roofs and roofing needs of customers using its services].) Other jurisdictions considering this issue have also found that the party claiming that a compilation of information is a trade secret must demonstrate the novel or unique nature of the compilation. (*See, e.g. United States v. Nosal* (9th Cir. 2016) 844 F.3d 1024, 1043 ["the nature of the trade secret and its value stemmed from the unique integration, compilation, and sorting of" the information contained in the source lists.]; *Woo v. Fireman's Fund Insurance Co* (2007) 134 Washington App. 480, 488-489 [same]; *OTR Wheel Engineering, Inc. v. West Worldwide Services, Inc*. (2015) WL 11117430, [*46] at *1 (E.D. Wash. Nov. 30, 2015) ["The use of commonly available material in an innovative way can qualify as a trade secret [but] to qualify for protection as a trade secret, however, the combination must still be shown to have novelty and uniqueness."].)

After applying the foregoing standards, this *Ruling* concludes that Moving Parties have failed to establish that the trip data as a whole, or any subcomponent thereof, is either novel or unique. Absent from the Rosenthal, Golde, Donahue, and Sipf Declarations is any explanation of the uniqueness of the disclosure of data that reveals a TNC trip that originates in zip code or census block x and terminates in zip code or census block y on date and time z. Moving Parties cannot provide such an explanation because zip codes and census blocks are geographic locations created by the Federal Government, rather than the TNCs (*See* Lyft's *Motion*, Exhibit A, which provides excerpts from the United States Census Bureau), and the Moving Parties are compiling the information in the manner dictated by the Commission. As such, populating fields by zip code and/or census block, or by any of the other categories included in the Annual Reports, does not make the information novel or unique.

Rather than setting forth the predicate facts for a novelty or uniqueness claim, at best, what the Sipf, Rosenthal, Golde, and Donahue Declarations explain are internal storage and use procedures for their companies' trip data. (Sipf Decl., ¶ ¶ 13 ["In addition to using its confidential data to develop new products and features, Uber also uses its data to design incentives to attract and retain users on the Uber Platform."] and 18 ["The information is stored on secure servers that are password protected."]; Rosenthal Decl, ¶¶ 6 ["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 10 ["Lyft stores the Census Block Trip Data on a secure software network protected by appropriate computer security controls[.]"; Donahue Decl., ¶ 6 ["HopSkipDrive is continuously evaluating trip data—including the detailed geolocational and other trip-specific data being requested in the annual report—to evaluate how customers use the platform and to improve its service offerings."]; and Golde Decl., ¶ 15 trip data is "protected through a secure information technology network[.]") But the Commission has not ordered the TNCs to produce what they term are proprietary databases—just the actual trip data itself in the manner dictated by the Commission.

Similar broad-based claims have been rejected as insufficient to satisfy the uniqueness standard for a trade secret claim. For example, in *Woo v. Fireman's Fund Insurance Co* (2007) 137 Wn. App. 480, 488-489, the Court rejected the assertion that an insurance claims manual was trade secret protected because of the unique manner in which it was assembled and utilized since the supporting declarations were too general:

> It is true that the use of commonly available materials in an innovative way can qualify as a trade secret, and the proponent of a trade secret "need not prove that every element of an information compilation is unavailable elsewhere." *Boeing Co. v. Sierracin Corp.*, 108 Wn.2d 38, 50, 738 P.2d 665 (1987). But to qualify for protection as a trade secret, the combination must still be shown to have "novelty and uniqueness." *Machen, Inc. v. Aircraft Design, Inc.*, 65 Wn. App. 319, 327, 828 P.2d 73 (1992), *overruled on other grounds by Waterjet Tech., Inc. v. Flow Int'l Corp.*, 140 Wn.2d 313, 323, 996 P.2d 598 (2000).
>
> The declarations of the claims managers are too conclusory to prove that the claims manuals compile information in an innovative way. The declarations do not supply any concrete examples to illustrate how the strategies or philosophies of Fireman's Fund claims handling procedures differ materially from the strategies or philosophies of other insurers.

As the declarations in the *Woo* decision failed to do, the Sipf, Rosenthal, Golde, and Donahue Declarations also fail to provide any concrete examples of how each TNC's business strategies or marketing philosophies differ from the other TNCs. For example, the Rosenthal Declaration states:

> Lyft can gauge the effectiveness of those incentives in 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.[32]

Yet the Rosenthal Declaration fails to demonstrate that Lyft's business practices and data analytics are any different from the practices and analytics employed at other TNCs, or that no other TNC utilizes such practices and analytics. In fact,

[32] Rosenthal Decl., ¶7.

the other Moving Parties' Declarations make claims similar to Lyft's. (Sipf Decl., ¶¶ 8, 9, and 10; Golde Decl., ¶ 13; and Donahue Decl., ¶ 6.)

When competitors engage in the same or similar processes to recruit potential customers and drivers, a claim that trip data information is either novel or unique may be questionable. In *American Paper & Packaging Products, Inc. v. Kirgan* (1986) 183 Cal.App.3d 1318, 1326, the Court addressed this issue in a slightly different context (*i.e.*, use of customer lists):

> The compilation process in this case is neither sophisticated nor difficult nor particularly time consuming. The evidence presented shows that the shipping business is very competitive and that manufacturers will often deal with more than one company at a time. There is no evidence that all of appellant's competition comes from respondents' new employer. Obviously, all the competitors have secured the same information that appellant claims and, in all likelihood, did so in the same manner as appellant--a process described herein by respondents.

A similar outcome is warrant by the current facts. A comparison of the Rosenthal, Sipf, Donahue, and Golde Declarations that were submitted in support of their clients' separate *Motions* reveals that all four declarants make similar claims about how their respective TNCs utilize trip data to further their business operations: (1) the TNCs compete against each other in terms of earning opportunities, app functions, and customer service; and (2) the TNCs develop new products and features through their use of the trip data to make rides more attractive to customers and drivers (Sipf Decl., ¶¶ 3 and 4; Rosenthal Decl., ¶¶ 7 and 8; Nomad's *Motion*, at 10; and Donahue Decl., ¶¶ 7 and 8.) While the internal data analytic process may vary at each company, each TNC is engaging in similar processes of utilizing trip data to attract customers, improve

customer service, and maintain or improve their competitive advantage over the same pool of potential TNC passengers and drivers.

Another flaw in Moving Parties' uniqueness argument is that they fail to establish, beyond generalized claims in the Sipf, Rosenthal, Golde, and Donahue Declarations, that any TNC competitor would want another TNC's trip data. For example, the *Woo* Court rejected the trade secret claim that its claim manual was unique, finding that there was no concrete evidence that a competitor would want to utilize the claim manual, as well as the financial benefit that a competitor would realize:

> The declarations provide no proof that any rival company would want to copy the manuals, nor do they quantify in any meaningful way the competitive advantage that the hypothetical plagiarizer would enjoy. *See Buffets, Inc.*, 73 F.3d at 969 (restaurant chain asserting trade secret protection for fried chicken recipes did not demonstrate any relationship between competitors' lack of success and unavailability of the recipes).

Similarly, the Sipf, Rosenthal, Golde, and Donahue Declarations provide no proof, other than speculation, that a rival TNC would want access to a rival's TNC databases and how much revenue or market share the rival TNC would realize. At best, the Declarations claim that TNC competitors "could and would analyze and manipulate that data" (Rosenthal Decl., ¶ 8), or "could exploit that information" (Sipf Decl., ¶ 12), but fail to provide any facts to back up their conclusions.[33]

[33] This *Ruling* acknowledges that there have been other out of state and federal decisions that have found that some of the trip data categories at issue here are trade secret. But this *Ruling* declines to follow these authorities as their findings are too conclusory and do not contain an application of the novel and uniqueness standard. (*See Rasier-DC, LLC v. B&L Service, Inc.* 2018 Fla.App. LEXIS 320; 43 Fla. L. Weekly D 145; 2018 WL 354557 [the aggregate trip data was not a

Footnote continued on next page.

There is an additional problem that undermines Moving Parties' trade secret argument--it is overbroad. They speak of proprietary databases, algorithms, and formulas used internally to develop strategies for appealing to customers and drivers, and to compete with other TNCs that will be compromised if trip data were publicly disclosed. (Sipf Decl., ¶ 6 ["pricing algorithms for rides"]; and ¶¶ 8 and 9 [Uber is developing "new products and features"]; Rosenthal Decl., ¶¶ 6 and 7 [trip data stored in "proprietary databases" and compiled for "business analytics purposes"]; Donahue Decl., ¶ 6 ["HopSkipDrive is continuously evaluating trip data—including the detailed geolocational and other trip-specific data being requested in the annual report—to evaluate how customers use the platform and to improve its service offerings."]; and Golde Decl., ¶¶ 12 ["Nomad's services in the State of California are all shared ride services, which use Via's proprietary algorithms[.]" and 15 ["Information about the algorithms and their inputs is closely guarded within Nomad and its parent company, Via."].) But the Commission has not asked Moving Parties to produce their internal analyses, algorithms, or business strategies for marketing their businesses. Instead, the Commission has ordered Moving Parties to produce their resulting data in the matter dictated by the Commission.

---

trade secret, but the granular trip data was trade secret protected from public disclosure]; *Ehret v. Uber Technologies, Inc*. 2015 U.S. Dist. LEXIS 161896 [court granted motion to seal information about the number of TNC trips taken during the proposed class period]; *Lyft, Inc. v. Pennsylvania Public Utility Commission* (2015) 145 A.3d 1235; 2016 Pa. Commw. LEXIS 374 [aggregated trip data that does not reveal details about individual trip locations is not trade secret]; and *Philliben v. Uber Technologies* 2016 U.S. Dist. LEXIS 193536; 2016 WL 9185000, settled by *McKnight v. Uber Techs. Inc*. 2017 U.S. Dist. LEXIS 124534 (N.D. Cal. August 7, 2017) [number of Uber riders who have used the Safe Rides Fee service, frequency with which Uber riders use the Uber App, revenue information, and information related to safety-related expenditures et the compelling reason standard for nondisclosure].)

Courts have recognized the distinction between a secret formula possibly being a trade secret and the resulting data derived from a secret formula. In *Cotter v. Lyft, Inc.* (N.D. Cal. 2016) 193 F.Supp.3d 1030, 2016 WL 3654454, at *2, the Court explained that while the uniquely developed formula might be protected, the resulting data is not trade secret protected:

> While the algorithms and proprietary price models that Lyft uses to set its fares and the rate of Prime Time premiums and, in turn, its commissions from those moneys are trade secrets, the bare output of those algorithms and price modes (*i.e.*, the total amount of commissions taken) is not. Though the manner in which Lyft determines its pricing is an important part of its competitive strategy, its revenue is not strategy but rather the result of that strategy.

(*See, also, Buffets, Inc. v. Klinke* (9th Cir. 1996) (Washington law) 73 F.3d 965, 968 ["This is not a case where material from the public domain has been refashioned or recreated in such a way so as to be an original product but is rather an instance where the end-product is itself unoriginal."].) Accordingly, this *Ruling* rejects the overbroad nature of Moving Parties' trade secret assertions.

Since Moving Parties have failed to satisfy the first element of a trade secret claim, it ordinarily would not be necessary for this *Ruling* to consider the balance of Moving Parties' trade secret arguments. However, as this *Ruling* will, in all likelihood, be appealed, this *Ruling* will address the balance of the claims so that the Moving Parties, as well as the Commission, have a complete understanding why the trade secret claim must be rejected in its entirety.

4.1.2. Moving Parties Fail to Establish that Trip Data has Independent Value Because of its Alleged Secrecy

In *DVD Copy Control, supra,* 31 Cal.4th, at 881, the California Supreme Court recognized that "trade secrets are a peculiar kind of property. Their only

value consists in their being kept private. Thus, the right to exclude others is central to the very definition of the property interest." (*See also Silvaco Data Systems v. Intel Corp*. (2010) 184 Cal.App.4th 210, 220-221 ["the *sine qua non* of a trade secret, the, is the plaintiff's possession of information of a type that can, at the possessor's option, be made known to other, ow withheld from them….Trade secret law, in short, protects only the right to control the dissemination of information."].) The secrecy adds to the trade secret's value 'because it is unknown to others." (*AMN Healthcare, Inc. v. Aya Healthcare Services, Inc*. (2018) 28 Cal.App.5th 923, 943.) In other words, the secrecy of the trade secret information provides the holder of the trade secret with "a substantial business advantage." (*Morlife, Inc. v. Perry, supra,* 56 Cal.App.4th, at 1522.)

Finally, in determining if a trade secret has independent value, the fact finder must consider if the claimant established the amount of time, money, or labor that was expended in developing the trip data, as well as the amount of time, money, or labor that would be saved by a competitor who used the trip data. (Judicial Council of California Civil Jury Instruction 4412 (Independent Economic Value Explained.) In *Yield Dynamics, Inc. v. TEA Systems* (2007) 154 Cal.App.4th 547, 564-565, the Court provided guidance as to the specificity of the showing to demonstrate independent value:

> Merely stating that information was helpful or useful to another person in carrying out a specific activity, or that information of that type may save someone time, does not compel a fact finder to conclude that the particular information at issue was "sufficiently valuable . . . to afford an . . . economic advantage over others." (Rest.3d Unfair Competition, § 39.) The fact finder is entitled to expect evidence from which it can form some solid sense of *how* useful the information is, *e.g.*, *how much* time, money, or

> labor it would save, or at least that these savings would be "more than trivial."

The *Ruling* must address whether Moving Parties carried their burden of establishing the independent value of its trip data because of its alleged secrecy.

Each Moving Party's showing lacks the necessary specificity to satisfy the second criterion of a trade secret claim and instead relies on the same two-part argument. First, each declaration contains language suggesting that the trip data is essential to the development and marketing of each TNC's operations. (Sipf Decl., ¶ 9 ["When developing new products and features, our product developers and engineers rely on the unique data that Uber has invested in collecting and developing over time from rider and driver use of the app."]; Rosenthal Decl., ¶ 7 ["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 vehicle supply."]; Golde Decl., ¶ 13 [Nomad claims that the release of trip date would "include highly detailed data about Nomad's trips which could reveal trade secrets by disclosing the logic behind the algorithms' ability to efficiently match riders with drivers and route multiple passengers sharing rides."] and Donahue Decl., ¶ 6 ["As with any business operating in the marketplace, HopSkipDrive strives to improve and differentiate its service offerings. HoSkipDrive does this in part by using the data and information that it collects as part of its operation[.]".)

Second, each declaration explains the potential impact on its employer's competitive advantage if the trip data were publicly disclosed. (Sipf Decl., ¶ 12 ["If Lyft or other competitors and potential competitors had access to Uber's competitively sensitive information, including information about Uber's product

mix, use of its Pool feature, or other information, these competitors could exploit that information to better compete against Uber."]; Rosenthal Decl., ¶ 8 ["If Lyft's competitors…were provided access to Lyft's Census Block 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, and other critical aspects of its business that it does not publicly disclose."]; Golde Decl., ¶ 13, quoted above; Donahue Decl., ¶ 10 ["[C]ustomers could use this information to seek and target drivers who utilize HopSkipDrive's platform and/or to determine our business strategies."

When read together, the declarations suggest that each TNC keeps its trip data secret, and that the secrecy allows each TNC to evaluate the effectiveness of its business promotions and to make upgrades as needed to provide a competitive TNC service to the riding public. In each declarant's view, a TNC's ability to remain competitive would be lost if its trip data would be made public because competitors would gain insights into a TNC's market share, pricing practices, marketing strategies, and other aspects of a TNC's business.

But even if the foregoing were accepted as true, the Sipf, Rosenthal, Golde, and Donahue Declarations fail to establish how the release of the trip data would lead to the loss of the trip data's independent value. First, they fail to quantify the independent value of each TNC's trip data or the unfair competitive advantage, except in the most generalized terms. (Sipf Decl., ¶ 4 ["[E]ach company invests substantial sums developing new products and features for riders and drivers, marketing to drivers and riders, and engaging in efforts to improve riders' wait times and drivers' earning."]; Rosenthal Decl., ¶ 6 ["Trip data is captured using data collection, analysis and reporting processes developed by Lyft over time and at great effort and expense."]; Golde Decl., ¶ 12

["Our algorithms are confidential and proprietary trade secrets results from a significant investment or our resources."]; and Donahue Decl., ¶ 7 ["HopSkipDrive has invested significantly in growing its business and service offerings."].) Instead, the language used is too generalized to permit the Commission to evaluate each TNC's claim, thus falling short of the evidentiary showing required by the *Yield Dynamics* decision.

Second, trip data does not disclose the business and service offerings, such as the driver incentive programs deployed during that period, or the driver acquisition programs and passenger promotions that the declarants tout. The Commission has not required any TNC to include in the Annual Report any information about driver incentive and/or acquisition programs, as well as passenger incentives and promotions. All the release of the trip data would show is that a passenger requested a TNC ride from zip code x and that the ride terminated in zip code y on z date and time. That information would not reveal why the passenger requested the trip on that day or why the passenger traveled to the destination zip code y. The trip data in the Annual Report does not have a column indicating whether the passenger took advantage of a passenger promotion a TNC advertised on that day or time, or if the passenger even knew of the passenger promotion. There could be other reasons why the passenger picked that particular trip that have nothing to do with a TNC's passenger promotions. For example, a passenger may decide to take a trip because of a special occasion (*e.g.,* date, engagement with friends, movie night, going to an entertainment venue), or need to take a trip because of employment obligations, and either or both scenarios could be completely unrelated to a TNC's passenger promotions. Thus, the release of the trip data will not provide any insights into a TNC customer's reason for requesting a trip, even if a competitor were to cross

reference the TNC's ride numbers against the TNC's passenger promotions run at that time the trip was requested.

Similarly, the release of TNC trip data will not reveal any secrets about TNC drivers or driver incentive programs deployed. As with the passenger trip data, the Commission has not required any TNC to reveal why a driver decided to log onto a TNC app or why the TNC driver decided to pick up a particular passenger and take that passenger to a particular zip code or census block. As the Commission does not require any TNC to provide personally identifiable information about TNC drivers, there would be no way for a competitor to gain any insights about the driving habits, patterns, or TNC-generated driving incentives. As with passengers, there could be other reasons why the TNC driver picked a particular day or time to log onto the TNC app or to select particular zip codes to pick up a TNC passenger that have nothing to do with a TNC's driver incentive program. The TNC driver could be working part time and the period in which the driver logged onto the TNC app may be the only available time in which to do so given the personal or professional constraints in the driver's life. If the trip data were released, there would be no way to know what motivated a TNC driver to log on to the TNC app for any particular ride or time.

Nor do the Moving Parties provide any credible rationale that their competitors could or would use the released trip data to their disadvantage. Each declarant claims that with the release of the trip data, competitors would be in a better position to compete since the TNC could manipulate the data and gain insights into a TNC's market share, marketing strategies, and other critical aspects of a TNC business operations that the TNC does not publicly disclose. (Sipf Decl., ¶ ¶ 12 and 15; Rosenthal Decl., ¶ 8; Golde Decl., ¶ 8; and Donahue

Decl., ¶ 13.) Moving Parties conclude that releasing the trip data will enable competitors to increase their ridership market share in California. (*See* Sipf Decl.,¶ 5.)

This *Ruling* rejects Moving Parties' argument for several reasons. First, trip data does not include pricing practices (outside the price of particular ride), marketing strategies, or other critical aspects of a TNC's business so it is speculative as to what insights would be revealed by the trip data's disclosure. All that would be revealed is the resulting data, which courts have found does not constitute a trade secret. Second, the claim that other TNCs licensed in California would want a competitor's trip data is speculative at best. Moving Parties refer to their competitors but fail to explain with any firsthand knowledge why these competitors would, in fact, want another TNC's trip data or gain any insights upon receipt. For example, the Uber's Sipf Declaration references "companies such as Wingz and Silver Ride, in addition to five TNCs approved for the transport of minors such as HopSkipDrive." (Sipf Decl., ¶ 5.) Yet the Sipf Declaration fails to provide any evidence that these presumed rival TNCs are actually trying to gain access to Uber's trip data who would in fact gain any benefit from the release that they don't already know. The Sipf Declaration also references Lyft as Uber's primary competitor who compete on "price and wait times…as well as app functionality and customer service." (Sipf Decl., ¶ 4.) While there is no doubt that Lyft is Uber's primary competitor as Uber and Lyft occupy over 99% of the California TNC market,[34] Uber has not demonstrated that Lyft has tried to get or even wants Uber's trip data.

[34] D.20-03-014, at 15.

Lyft makes a similarly vague and factually unsupported argument regarding competitors wanting the Lyft trip data. The Rosenthal Declaration identifies Lyft's competitors as including "Uber, HopSkipDrive, Wing[z], Silver Ride, Nomad Transit, and any other company that has obtained or might wish to obtain a TNC permit from the Commission" who would benefit from the release of Lyft's trip data. (Rosenthal Decl., ¶ 8.) Yet, Lyft fails to set forth any facts that any of its competitors would want, or has tried to obtain, Lyft's trip data. The Rosenthal Declaration underscores this point when he states: "I am aware that Lyft has been approached by at least one company, *who is not a competitor*, which has inquired about purchasing access to anonymized trip data, or portions thereof." (Rosenthal Decl., ¶ 9, italics added.) Rather than identifying a rival TNC by name, the reference that Lyft does make is to "an active market that has developed for the sale or licensing of such data." (*Id.*)

The claims by the two smaller TNCs that are seeking to prevent the disclosure of their trip data are equally vague. HopSkipDrive does not identify a competitor by name and instead claims "if competitors had access to HopSkipDrive's customer data from California, they could identify our customers who book rides and target those customers with competitive offers." (Donahue Decl., ¶ 8.) Nor does Nomad, who has elected to piggyback on Uber, Lyft, and HopSkipDrive's nonspecific "legal arguments and factual assertions explaining the trade secret nature of certain information in the Annual Reports. (Nomad's Motion, at 9.) Moreover, instead of identifying a competitor, Nomad asserts in its *Motion* that "if competitors learned the algorithms' logic and were able to assess them using detailed trip data, they would be able to revers engineer and copy them to better compete with Nomad and Via, whether in direct-to-consumer shared ride services or in competitive procurements for

Transit Tech solutions with public and private partners. (Nomad's *Motion*, at 10.) but by its own admission, Nomad is, at present, a small venture that "currently operates in only one deployment in California: a service in partnership with the City of West Sacramento." (*Id.*, at 3, footnote 3.) Nomad fails to demonstrate that any other licensed TNC has an interest in learning about Nomad's West Sacramento operations.

Uber and Lyft's arguments are even less persuasive when we look at the smaller TNC operations that have been identified as competitors. HopSkipDrive primarily transports minors,[35] Silver Ride specializes in providing rides for senior citizens,[36] Nomad focuses on a small set of riders, with certain services allowing only "select and limited groups of riders in a specific geographic area,"[37] and Wingz began as an airport service but has since branched into providing a niche service to specialty events, doctor's appointments, and other destinations.[38] But the Annual Reports do not require a TNC to list a driver's age as part of the trip data template so it is not clear what use HopSkipDrive and Silver Ride would have for another TNC's trip data. It is also not clear how limited operations such as Nomad and Wingz would want Uber and Lyft's trip data which would cover their statewide operations. As for the "any other company that has obtained or might obtain a TNC permit" that the Rosenthal Declaration references,[39] as well as the "potential competitors" that the

[35] Donahue Decl., ¶ 2 ("HopSkipDrive is a very small TNC…that focuses on arranging safe rides for kids and other individuals who need a little extra support.")

[36] *Id.*

[37] Golde Decl., ¶ 5.

[38] https://wwwlwingz.me

[39] Rosenthal Decl., ¶ 3.

Sipf Declaration references,[40] these claims are too ambiguous and speculative to warrant further consideration as they don't satisfy the granularity of information standard that the Commission adopted in D.20-03-014 for establishing confidentiality claims. As such, this *Ruling* concludes that Moving Parties have failed to explain how any of their competitors would benefit by receiving trip data that would be to the detriment to whatever independent economic value the trip data has.

The Commission has seen courts reject similarly generalized assertions as being factually insufficient to support a claim of trade secret. In *Confederated Tribes of Chehalis Reservation v. Johnson* (1998) 135 Wn.2d 734, 749, the Court stated:

> Through general statements in declarations, the Tribes maintain that their competitors would gain an advantage over them if the amount of the two percent community contributions were made public. In the Tribes' view, a potential competitor could use the two percent figure to calculate gross revenue and then could gauge the market and market saturation. Therefore, the Tribes argue, the information derives economic value from not being generally known.
>
> However, there is no evidence in the record before us that knowledge of a casino's profitability could not be generally ascertained by visiting the casino site, through newspaper articles about the casino, or through employees, tribal members, or local service agencies which are recipients of community contributions. Even if the information were not readily ascertainable, there is no evidence in the record to support the Tribes' contention that the information derives "independent economic value" from not being generally known.

[40] Sipf Decl., ¶ 5.

Courts have also refused to recognize prices or fees as having independent economic value when different variables can go into calculating the price or fee. In *Belo Management v. Click!Network* (2014)184 Wn.App. 649, 658, the Court stated:

> Similarly, here, the broadcasters' allegations of harm are too conclusory and speculative. They make the same argument as the firm in Robbins: Release of this information would give competitors an unfair advantage. This reason alone is insufficient to prove that the information is a trade secret. The broadcasters have not proven that their prices have independent economic value to their competitors or other cable systems. As the broadcasters concede, every negotiation is different. Markets and cable systems vary. Prices fluctuate over time. Thus, it does not follow that the other cable systems could viably argue that they are entitled to the same price as a cable system in a different market during a different time period.

A price for a trip that is revealed through the release of trip data would not be of any use to another TNC because Annual Reports do not require TNCs to explain how the price of a trip was calculated or if any special promotions were offered. A rival TNC would still have to conduct its own analysis and use whatever algorithms it has developed to best determine what price to charge for a comparable ride. Accordingly, just as the Court found in *Belo*, the TNCs' claims of economic harm are conclusory and speculative.

Finally, this *Ruling* rejects Lyft's attempts to rely on secondary sources to establish its claim that the trip data has acquired independent value. Lyft cites to articles and company named Datarade that allegedly analyze the monetary value of mobility data. (Rosenthal Decl., ¶ 9.) The problem with Lyft's position is that it has failed to establish the admissibility threshold for the Commission to consider these materials. D.20-03-014, OP 2.h. orders any TNC claiming

confidentiality as to any of the data in its Annual Reports from 2020 and onward must submit a declaration under penalty of perjury that substantiates the claim:

> The TNC must provide a declaration (executed with personal knowledge and under penalty of perjury) in support of the legal authority relied on to support the confidentiality claims for Government Code §§ 6254(k) and 6255(a), General Order 66, Civil Code §§ 3426 through 3426.11, Government Code § 6254.7(d), and any other statute, rule, order, or decision that the TNC is relying upon to support each claim of confidentiality.

Lyft has not met that evidentiary showing. Lyft failed to submit any declarations from the authors of these reports and studies. Mr. Rosenthal is not the author of the reports and studies, nor is he an employee of Datarade, so he cannot authenticate them. He even prefaces his argument with the qualifier "it is my understanding and belief," meaning he lacks personal knowledge of any of the claims made in that paragraph of his Declaration. While it is true that the generally the technical rules of evidence need not be applied in hearings before the Commission,[41] D.20-03-014 has imposed a higher evidentiary standard to substantiate a confidentiality claim, and Lyft has failed to meet that enhanced evidentiary showing. Thus, these articles and reports will not be considered by this *Ruling* as they fail the admissibility standard.

This conclusion not to consider these secondary sources is also driven by the fact that Lyft's argument is simply that—an argument based on what is known in California law as inadmissible hearsay. Evidence Code §1200 defines hearsay as follows:

> a. "Hearsay evidence" is evidence of a statement that was made other than by a witness while testifying at the

[41] Rule 13.6.

hearing and that is offered to prove the truth of the matter stated.

b. Except as provided by law, hearsay evidence is inadmissible.

c. This section shall be known and may be cited as the hearsay rule.

If an out of court statement is being offered for the truth of the matter asserted, and that statement does not fit within one of the statutorily recognized exceptions to the hearsay rule (*i.e.*, "[e]xcept as provided by law"), that statement is inadmissible hearsay. (*People v. Smith* (2016) 63 Cal.4th 665, 674 ["Thus, a hearsay statement is one in which a person makes a factual assertion out of court and the proponent seeks to rely on the statement to prove that assertion is true. Hearsay is generally inadmissible unless it falls under an exception. (Evid.Code, § 1200, subd. (b).)]."") As Lyft is offering these studies for the truth of the matter asserted (*i.e.*, that trip data can be manipulated to reveal private information about a TNC passenger) and no explanation has been offered for why the authors of the studies could not provide declarations or show that the studies somehow fit within a hearsay exception, the studies are inadmissible hearsay under California law.

The outcome is the same in proceedings before the Commission, notwithstanding the fact that the Commission utilizes a more relaxed evidentiary admissibility standard. In *Utility Reform Network v. Public Utilities Commission* (2014) 223 Cal.app.4th 945, the Court of Appeal addressed the question of the Commission's ability to accept and rely of hearsay evidence as the sole support for its finding on a disputed issue of material fact. To prove the need for a new gas fired power plant known as the Oakley Project, Pacific Gas and Electric Company (PG&E) presented a declaration from an executive of the

California Independent System Operator (the CAISO) and a petition the CAISO had filed with a federal agency. Neither the CAISO executive nor the authors of the petition testified in the Commission's proceedings. While the assigned ALJ would not consider this evidence because it was inadmissible hearsay, the Commission voted in an alternative decision to admit the evidence and found that there was a need for the Oakley Project.

In resolving the evidentiary objection to relying on evidence from a person who was not present at the hearing, the Court of Appeal noted that there is a distinction between the admissibility and substantiality of hearsay evidence, citing to *Gregory v. State Board of Control* (1999) 73 Cal.App.4th 584, 597. *Gregory* explained that hearsay "is evidence of a 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." (*Id.*, at 596; and Evidence Code, § 1200, subd. (a).) 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[.]" (*Id.*, citing to *Funke v. Department of Motor Vehicles* (1969) 1 Cal.App.3d 449, 456. The Commission has found in prior decisions that it would not rely on the hearsay opinions of unavailable experts. (*Cleancraft, Inc. v. San Diego Gas and Electric Co.* (1983) 11 Cal.P.U.C.2d 975, 984 [unsubstantiated hearsay not sufficient on its own to establish an essential fact.) Thus, for the Commission to rely on hearsay evidence, the evidence must first pass the admissibility test.

This *Ruling* finds the Commission's decision in *Cleancraft* to be applicable here and concludes that the unsworn reports that Lyft references in the *Appeal* fail the admissibility test. Lyft is asking the Commission to accept the opinions of authors who are supposedly experts in the field of data manipulation and extrapolation, none of whom provided declarations under oath. Lyft offers no

explanation why it couldn't obtain declarations from these authors, especially since they would have been offered to resolve a disputed issue—whether trip data is a trade secret. Thus, this *Ruling* rejects Lyft's request to admit and consider these unsworn reports as they are not the type of evidence the Commission is accustomed to relying upon to resolve a disputed issue of material fact.

Second, even if the unsworn hearsay reports were admissible, this *Ruling* would not give the reports any weight because they fail the substantiality test. In *Utility Reform Network*, the Court offered the following guidance:

> As the California Supreme Court has explained, "mere admissibility of evidence does not necessarily confer the status of `sufficiency' to support a finding *absent other competent evidence*." (*Daniels v. Department of Motor Vehicles* (1983) 33 Cal.3d 532, 538, fn. 3 [189 Cal.Rptr. 512, 658 P.2d 1313], italics added (*Daniels*).) "There must be substantial evidence to support ... a board's ruling, and hearsay, unless specially permitted by statute, is not competent evidence to that end." (*Walker v. City of San Gabriel* (1942) 20 Cal.2d 879, 881 [129 P.2d 349] (*Walker*), overruled on another ground in *Strumsky v. San Diego County Employees Retirement Assn.* (1974) 11 Cal.3d 28, 37, 44.[42]

California Courts refer to the substantiality test as the "residuum rule," under which the substantial evidence supporting an agency's decision must consist of at least "a residuum of legally admissible evidence. (223 Cal.App.4th, at 960-961.)

This *Ruling* is tasked with ruling on Lyft's *Motion* must determine if there is other competent substantial evidence to support Lyft's contention that trip data is a trade secret because it has independent value because of its secrecy, and the answer is no. As this *Ruling* explained, *supra*, the flaws in the Rosenthal

[42] 223 Cal.App.4th, at 960.

Declaration are fatal to Lyft's assertion that trip data is trade secret protected. And there is no other admissible evidence to support Lyft's position.

According, this *Ruling* finds that all of the Moving Parties have failed to establish the second criterion of a trade secret claim for their trip data.

4.1.3. Moving Parties Fail to Establish that they have Taken Reasonable Efforts to Maintain the Secrecy of their Trip Data

A person or entity claiming a trade secret must also demonstrate that the claimant made "efforts that are reasonable under the circumstances to maintain its secrecy. (*In re Providian Credit Card Cases* (2002) 96 Cal.App.4th 292, 304.) The Court went further to explain why the absence to maintain the secrecy of a trade secret dooms a trade secret claim:

> Public disclosure, that is the absence of secrecy, is fatal to the existence of a trade secret. "If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished." (*Ruckelshaus v. Monsanto Co.* (1984) 467 U.S. 986, 1002; *see* Legis. Com. com., 12A West's Ann. Civ. Code (1997 ed.) foll. § 3426.1, p. 238 ["the trade secret can be destroyed through public knowledge"]; 1 Milgrim on Trade Secrets (2001) § 1.05[1], p. 1-197 ["unprotected disclosure . . . will terminate . . and, at least prospectively, forfeit the trade secret status"].)

In determining if reasonable efforts to protect a trade secret's secrecy have been made a court can consider the following factors: whether documents or computer files containing the trade secret were marked with confidentiality warnings; whether the claimant instructed the employees to treat the trade secret as confidential; whether the claimant restricted access to the trade secret; whether the trade secret was kept in a restricted or secured area; whether employees had to sign a confidentiality or nondisclosure agreement to access the

trade secret; and the extent to which any general measures taken would prevent the unauthorized disclosure of the trade secret.[43]

Moving Parties fail to satisfy the reasonable efforts standard. Each declarant identifies all or some of the following efforts to maintain the confidentiality of trip data: (1) the data is stored on a secure software network or through other protective means (Sipf Decl., ¶ 18; Rosenthal Decl., ¶ 10; Golde Decl., ¶ 15; Donahue Decl., ¶ 17); (2) employees must sign a confidentiality agreement as a condition of employment or to be given access to trip data (Sipf Decl., ¶ 18; Rosenthal Decl., ¶ 10; Golde Decl., ¶ 15); (3) employees must sign an employee handbook which describes the employee's obligation to maintain the secrecy of confidential and proprietary information (Sipf., ¶ 18; Rosenthal Decl., ¶ 10); (4) all visitors to a TNC's headquarters must read and sign a non-disclosure agreement before proceeding past the reception desk (Rosenthal Decl., ¶ 10); (5) if trip data is shared with a third party not bound by confidentiality obligations, the trip data is provided in aggregated form and private partners must execute non-disclsoure agreements (Golde Decl., ¶ 15); and (6) TNCs only disclose trip data to regulators as required by law but makes every effort to ensure confidentiality protections are in place or the data is sufficiently obfuscated. (Sipf Decl., ¶ 19.)

The problem with the Moving Parties' declarations is their limited focus of employees, third parties, and regulators. The hole in their analysis is that no declarant addresses if TNC drivers are employees, and whether a TNC driver's and a passenger's access to trip data is dependent on them agreeing to maintain trip data confidentiality. As to the first point (*i.e.,* are TNC drivers' employees),

[43] CACJI No. 4404 (Reasonable Efforts to Protect Secrecy). Some of the factors from CACJI No. 4404 are listed in *Whyte v. Schlage Lock Co*. (2002) 101 Cal.App.4th 1443, 1454.

Uber and Lyft have consistently argued in its filings before this Commission and in civil actions filed in state and federal court that their drivers are independent contractors rather than employees. Most recently, in *People v. Uber Technologies, Inc., et al.*, (2020) 56 Cal.App.5th 266, 278, the Court found:

> The contracts between defendants and the drivers provide that the relationship between Lyft or Uber, on the one hand, and the drivers on the other, is not one of employment Rather, the "Platform Access Agreement" for Uber's "Rides" platform specifies that the parties' relationship "is solely as independent business enterprises, each of whom operates a separate and distinct business enterprise that provides a service outside the usual course of business of the other." Lyft's Terms of Service provide that the driver and Lyft 'are in a direct business relationship, and the relationship between the parties under this Agreement is solely that of independent contracting parties[.]

(*See also*, *Cotter v. Lyft, Inc.* (N.D. Cal. 2015) 60 F.Supp.3d 1067, 1070 ["The plaintiffs and Lyft have filed cross-motions for summary judgement, with the plaintiffs urging the Court to declare them 'employees' as a matter of law, and Lyft urging the Court to declare them 'independent contractors' as a matter of law."]; and *Comments of Zimride, Inc.* (now Lyft), at 4, filed on February 11, 2013 in this proceeding ["Zimride does not employ or compensate drivers[.]".)[44] TNCs consider their TNC drivers to be independent contractors, a point that the none of the declarants contradicts. HopSkipDrive and Nomad also claim that their drivers are independent contractors.

[44] On November 4, 2020, California voters passed Proposition 22, which gave TNC companies such as Uber and Lyft the right to classify their drivers as independent contractors: "an app-based driver is an independent contractor and not an employee or agent with respect to the app-based driver's relationship with a network company if the following conditions are met[.]"

As to the second point (*i.e.*, whether a TNC driver must maintain trip data confidentiality) the declarants are also silent. There is no reference to the Uber Platform Access Agreement or the Lyft Terms of Service to indicate that Uber or Lyft drivers are contractually bound to keep trip data secret. So, when a TNC driver logs onto the TNC's app in order to connect with a TNC passenger, the TNC driver knows what zip code from which the proposed ride originates and where it will terminate, and with that information the TNC driver can determine the census block from where the ride commences and terminates. The TNC driver will also know the date and time of the trip as well as the fare. To the extent a TNC has provided the TNC driver with advice on the best zip codes to travel to, as well as the best times of the day to work in order to maximize the number of passenger ride requests, that information is also in the TNC driver's possession. Likewise, to the extent a TNC has utilized driver incentive programs to secure more frequent TNC drivers, the drivers are aware of the incentive programs and are under no requirement to keep this information confidential.

Even more damaging to each TNC's secrecy claim is the fact that Moving Parties do not claim that a TNC's drivers may only work for that TNC, or that the driver may not use the learned trip data if the driver logs on to another TNC app to provide passenger services. In fact, it is not uncommon to see a TNC vehicle with both Lyft and Uber trade dress insignias. This means that a Lyft driver who has received the trip data described in the foregoing paragraph is free to transport that trip data and use it while driving for Uber or any other permitted TNC operation. There is also no impediment to a Lyft driver sharing the trip data with Uber or any other permitted TNC operation. Thus, Moving Parties' 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 TNC drivers are being provided with unrestrained access to alleged trade secret trip data.[45]

TNC passengers also have unrestricted access to a TNC's trip data as it relates to the trip that the passenger has contracted with the TNC driver to provide. Every passenger knows the originating and terminating zip codes (and by extension the census blocks) of every requested trip as well as the cost of the trip. To the extent the TNC passengers have chosen a particular ride as a result of a TNC passenger promotion, the passenger is not required to keep that information secret. The Sipf, Rosenthal, Golde, and Donahue Declarations do not claim that passengers logging on to the TNC app are required to execute a confidentiality agreement and not disclose the trip data information and incentives offered to induce the passenger to take a particular trip. To the contrary, TNC passengers are free to communicate their trip data knowledge to any other permitted TNC operation that they choose to patronize.

The United Sates Supreme Court explained in *Ruckelshaus*, *supra*, 467 U.S. at 1002, that such unrestricted access to and use of alleged trade secret information is fatal to establishing a trade secret claim: "If an individual discloses his trade secret to others who are under no obligation to protect the

[45] This Ruling is not swayed by the fact another Court reached a different conclusion. *City of Seattle, supra,* found that although TNC drivers possessed the beginning and ending zip codes for each trip driven, TNC drivers do not have access to the other information contained in the quarterly zip code reports. Thus, *City of Seattle* concluded that the fact the drivers possessed some of the information did not undermine the trade secret claim. This *Ruling* finds the Court's conclusion difficult to accept. The starting and ending zip code data for each trip are, in fact, part of the trip data information that Lyft and Rasier claimed was trade secret protected. Since the TNC drivers in Seattle and California have access to this and other trip data that Moving Parties do not want the Commission to publicly disclose, *City of Seattle* is unpersuasive in establishing that trip data qualifies as a trade secret.

confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished." (*See also DVD Copy Control*, *supra*, 31 Cal.4th, at 881 ["Once the data that constitute a trade secret are disclosed to others, or others are allowed to use those data, the holder of the trade secret has lost his property interest in the data."].) In sum, the TNCs' internal measures to limit employee access to trip data are insufficient to satisfy the reasonable efforts standard as "they are not designed to protect the disclosure of information" by the TNCs' drivers and passengers. (*Klinke*, *supra*, 73 F.3d, at 969.)

In conclusion, this *Ruling* finds that Moving Parties have failed to carry their burden of establishing each of the three elements of a trade secret claim.

4.1.4. Fare Factors

For the 2021 Annual Reports, CPED created a new reporting category called "fare factors." These are factors that go into the final fare such as base fare, cost per mile, cost per minute, maximum fare, minimum fare, cancel penalty, scheduled ride cancel penalty, schedule ride minimum fare, service fee, local fee, airport fee, surge pricing fee, prime time fee, applicable tolls, booking fee, cancellation fee, etc.). In requiring this information, CPED seeks to learn more about passenger fares by having them broken down by all the different fees that TNCs charge in addition to the mileage cost of the ride.

HopSkipDrive asks for confidential protection for fare factors on the grounds that this information is trade secret and its public disclosure would violate trade secret protection.[46] This *Ruling* rejects HopSkipDrive's request on the grounds that it fails to establish that fare factors meet the definition of a trade secret.

[46] HopSkipDrive *Motion*, at 12.

4.2. Balancing Test Considerations Weigh in Favor of Disclosing Trip Data

4.2.1. Evidence Code § 1060 and the Interplay with Government Code § 6254(k)

Gov. Code § 6254(k) provides an exemption for "Records, the disclosure of which is exempted or prohibited by federal or state law, including, but not limited to, provisions of the Evidence Code relating to privilege." The Evidence Code includes several privileges that a privilege holder may assert as a basis for refusing to provide evidence and, in certain cases, to prevent others from disclosing the information. Such evidentiary privileges include the trade secret privilege (Evidence Code §§ 1060-1061). If a state agency determines that certain information is subject to one of these privileges, or similar federal or state laws exempting or prohibiting disclosure, it may withhold information from its response to CPRA requests on the ground that such information is exempt from mandatory disclosure, pursuant to Gov. Code § 6254(k).

However, while evidentiary privileges such as the trade secret privilege are incorporated into the CPRA as potential bases for an agency to assert the Gov. Code § 6254(k) exemption, an assertion of the trade secret privilege by an entity that submits information to a governmental agency does not guarantee nondisclosure. A party asserting the trade secret privilege under Evidence Code § 1060 bears the burden of proving all the elements in that Code Section, which states as follows:

> If he or his agent (sic) or employee claims the privilege, the 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.

Thus, in addition to proving that information falls within the applicable statutory definition of a trade secret, one who wishes to avail of the privilege to refuse to disclose, and to prevent another from disclosing, asserted trade secret information, the moving party must prove that the "allowance of the privilege will not tend to conceal fraud or otherwise work injustice." If the Commission believes the latter, it is not required to honor the party's Evidence Code § 1060 trade secret privilege claim.[47]

Application of the foregoing test to Moving Parties Motions leads this *Ruling* to conclude that concealing Moving Parties' alleged trade secret protected trip data would work an injustice as there is a strong public interest in obtaining trip data. As the *2020 Confidentiality Ruling* found:

> There is a public interest in learning when riders are in operation and when trips are accepted or rejected. Public entities have an interest in knowing how many drivers are in operation on their rides for the planning purposes identified above, and would also want to know the number of times and when rides are accepted or rejected to determine if the TNC ride service is being provided to all neighborhoods in a nondiscriminatory manner. County district attorneys or the state attorney general may want to use this data to bring the necessary enforcement actions in civil court.[48]

The planning purposes that the *2020 Confidentiality Ruling* referenced are those identified in the Comments from the San Francisco Municipal Transit Agency, San Francisco County Transportation Authority, San Francisco City Attorney's Office, and the San Francisco International Airport *Opening Comments on Proposed*

---

[47] *See Uribe v. Howie* (1971) 19 Cal.App.3d 194, 205-207, and 210-211; and *Coalition of University Employees v. The Regents of the University of California* (Super. Ct. Alameda County, 2003, No. RG03-0893002) 2003 WL 22717384. In conducing the balancing test, the courts found that the public interest in disclosure outweighed the claimed need for secrecy.

[48] *2020 Confidentiality Ruling*, at 20-21.

Decision Re; Data Confidentiality Issues: trip data information is relevant in determining the impact of TNC services on their infrastructure, environmental impacts, traffic patterns, and the overall quiet enjoyment of their cities and counties.[49] In fact, Lyft put the question of the environmental and infrastructure benefits of TNC rides as basis for allowing them to operate when Lyft filed its initial *Comments* in this proceeding:

> Giving people viable and convenient alternatives in transportation – as a complement to public transit, taxis, carsharing, carpooling, etc. – is the critical element that makes reduced individual car ownership and use of single occupancy vehicles achievable. For platform-based communities to reach the critical mass tipping point at which they can significantly contribute to reduction of urban congestion, greenhouse gas emissions, and other problems caused by single-occupant driving, such communities must be allowed to develop and flourish without unnecessary or ill-fitting regulatory barriers.[50]

It would not be surprising for local government entities to want access to the trip data to evaluate whether the claimed environmental and infrastructure benefits from allowing TNC vehicles to operate have been realized. The San Francisco Municipal Transportation made such an argument in its *Comments* on Issue Track 3—Trip Data:

> San Francisco's transportation planners need TNC trip data to perform their duties. Under the City's charter, SFMTA has a responsibility to the general public to plan the transportation infrastructure for the future, manage congestion, and manage curb space appropriately. Without TNC data, SFMTA transportation planners must rely instead on anecdotal information to fill the gap, but such information does not

[49] *Id.*, at 19 and footnote 37.

[50] Zimride (now Lyft) *Comments*, filed February 11, 2013.

> present an accurate depiction of conditions on the ground. Creating public policy on factual, real time data, is clearly preferable. Here, the CPUC already requires TNCs to report much of the relevant data. Sound public policy requires the CPUC to make it available to allow local jurisdictions to make intelligent, supported transportation planning decisions for the benefit of all Californians.

In their Motions, none of the Moving Parties challenge the validity of the claims of municipalities for access to trip data that the *2020 Confidentiality Ruling* cited.

In a recent California decision, the Court of Appeal recognized a municipality's interest in obtaining a TNC's trip data goes beyond environmental and infrastructure matters. In *City and County of San Francisco v. Uber Technologies, Inc.* (2019) 36 Cal.App.5th 66, 73-74, the Court acknowledged that the San Francisco City Attorney has a broad right to investigate when it suspects an entity operating withing its jurisdiction is violating the law, citing to *California Restaurant Assn. v. Henning* (1985) 173 Cal.App.3d 1069, 1075. The San Francisco City Attorney claims it began its TNC investigation to determine:

- Whether Uber was violating the law in several areas relating to unsafe driving and illegal parking, the congestion and volume of Uber vehicles, inequality of access and treatment of passengers, and the distance driven by Uber drivers prior to commencing a shift, after media reports that Uber incentivizes drivers to drive as much as 200 miles or more before driving for an additional 12 to 16 hours, crowding the City's streets with unfamiliar and fatigued drivers.
- Whether Uber was violating California nuisance law, Civil Code § 3479, since the number of TNC vehicles might obstruct the free use of property so as to interfere with the comfortable enjoyment of life or property, or unlawfully obstruct the free passage or use, in the customary manner, of any public park, square, street, or highway.

- Whether Uber was failing to provide adequate accommodations for disabled riders and, possibly, in violation of the Unruh Civil Rights Acts (Civil Code § 51, subd. (b) and Civil Code § 54) and other state laws protecting individuals with disabilities.
- Whether Uber was underpaying its drivers and thereby violating San Francisco's independent minimum compensation ordinance (S.F. Administrative Code, ch. 12V).[51]

The Court found that the administrative subpoena seeking Uber's Annual Reports submitted to the Commission from 2013 to 2017, as well as the raw data the reports were based, was relevant to the City's investigations into possible violations of the law:

> The CPUC reports requests are reasonably relevant to the City's investigation of possible violation of state and municipal laws by Uber. (Citation omitted.) The CPUC reports contain information and data regarding safety problems with drivers, as well as hours and miles logged by drivers, which are relevant to the City Attorney's investigation of safety hazards, parking violations, and other possible violation of state nuisance law. The accessibility plans and the data on providing accessible vehicles included in the CPUC reports are clearly relevant to the City Attorney's investigation of possible violations of state law protections for individuals with disabilities.

The *Ruling* finds that public entities would also be interested in TNC trip data for all the foregoing reasons, and it would result in an injustice to deny the public access to this trip data. Based on the data provided in the Annual Reports, the TNC industry has been a rapidly growing mode of private transportation, accounting for more than millions of rides annually in California,

[51] 36 Cal.App.5th, at 74-75.

so TNCs reach and impact on municipalities where they conduct business is no doubt pervasive. Several investigations into whether a TNC such as Uber or 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.

Rather than challenge other government agencies' interests in obtaining trip data, Lyft claims, incorrectly, that the fact that other government agencies "might find Lyft's data useful for various purposes cannot justify denying confidential treatment to that data."[52] Lyft bases its position on a quote from *City of San Jose v. Superior Court* (1999) 74 Cal.Ap.4th 1008, 1018 wherein the Court stated the "the purpose of the requesting party in seeking disclosure cannot be considered." Lyft's argument is incorrect once City of San Jose is understood in its proper legal context as a case that did not construe Government Code § 6254(k). The City of San Jose filed opposition to the San Jose Mercury's petition for writ of mandate, which sought the production of citizen complaints about airport noise. In its opposition, the City of San Jose argued that the airport noise complainants' privacy interest in their personal information outweighed the public interest in disclosure of their names, addresses, and telephone numbers. If this personal information was disclosed, the complainants would be subject to harassment and intimidation, and the public's reporting of airport noise complaints would be chilled. When weighing the City of San Jose's right under Government Code § 6255 to refuse to produce records, the Court

[52] Lyft *Motion*, at 26.

said: "The burden of proof is on the proponent of nondisclosure, who must demonstrate a "clear overbalance" on the side of confidentiality. ([Govt. Code] § 6255; *Black Panther Party v. Kehoe* (1974) 42 Cal.App.3d 645, 657.) The purpose of the requesting party in seeking disclosure cannot be considered."[53] As such, the validity of the government's objection to a Freedom of Information Act request in *City of Jan Jose* did not turn on the resolution of the interplay between Government Code § 6254 and Evidence Code § 1060, statutes that do permit consideration of a third party's interest in obtaining government records.

In sum, this *Ruling* finds that it would work a manifest injustice if interested local entities were prohibited from gaining access to trip data.

4.2.2. Government Code § 6255

Government Code § 6255(a) is the catch-all provision which may be used for determining the confidentiality of records not covered by a specific exemption enumerated in the CPRA. This provision allows an agency to balance the public interest that would be served by withholding information with the public interest that would be served by the disclosure of the information. (*Humane Society of the United States v. Superior Court* (2013) 214 Cal.App.4th 1233, 1255.) To withhold information, the agency must find that the public interest served by not disclosing the record clearly outweighs the public interest served by the disclosure of the record. Under this CPRA balancing test, a submitter of information requesting confidential treatment under Government Code § 6255(a) "must identify the public interest and nor rely solely on private economic

[53] *See also U.S. Department of Justice v. Reporters Committee for Freedom of Press* (1989) 489 U.S. 749, 772: "Thus, whether disclosure of a private document under Exemption 7(C) is warranted must turn on the nature of the requested document and its relationship to "the basic purpose of the Freedom of Information Act to open agency action to the light of public scrutiny.'

injury." (D.17-09-023, at 44.) While the public's right to information in possession of the government must be construed broadly, *Humane Society* cautions that "exemptions are to be construed narrowly." (214 Cal.App.4th, at 1254.) Finally, although Government Code § 6255(a) references the "agency," suggesting that it is incumbent on the government entity holding the information to establish that the catch-all exemption applies, the burden of proof as to the application of an exemption is on the proponent of nondisclosure. (*Michaelis, Montanari & Johnson v. Superior Court* (2006) 38 Cal.4th 1065, 1071.) In this case, the burden would be on the TNCs to establish, by the preponderance of the evidence, the applicability of the catch-all exemption.

4.2.2.1. Does the Public Interest in Nondisclsoure Clearly Outweigh Disclosure?

This *Ruling* must first consider if the public interest in nondisclosure of the trip data clearly outweighs disclosure. As this catch-all exemption comes into play only if the confidentiality of records is not covered by a specific exemption enumerated in the CPRA, TNs cannot assert that the trip data is protected by the trade secret privilege. The question this *Ruling* must address is what proof the TNCs offered, beyond their claims of trade secret protection, to avail themselves of the catch-all exemption to prevent the disclosure of trip data. To do so, we must consider each TNC's Motion as different arguments are advanced.

- Lyft

In reviewing Lyft's *Motion,* Lyft raised the possibility that the trip data can lead to competitive companies and anyone gaining access to the trip data learning a rider's exact pick up and drop off addresses which could reveal personal information about the passenger (*e.g.*, gender, sexual predisposition, political affiliation, medical condition, *etc.*):

> Consider the revealing information one can learn with just a few details regarding a TNC ride, such as the precise time and general location at which the ride commenced. A spouse *might*, for example, ascertain the true destination of their partner after they leave the house; whether to the office located in one census block or zip code, or to a suspected paramour's residence, a healthcare or psychiatric facility, a political rally, or another suspected location in a different census block or zip code….Put simply, *it is impossible to anticipate*—and confidently dismiss—the virtually endless nefarious purposes to which such a massive, detailed, and content-rich database *might* be put. (Italics added.)[54]

In support of the arguments from its *Motion*, Lyft references a series of secondary source articles and informational maps from the US Census Bureau as its factual support.[55]

This *Ruling* rejects Lyft's argument for two reasons. First, the argument lacks support from a declaration under penalty of perjury with the necessary granularity required by D.20-03-014, OP 2.h. None of the authors of the various studies that Lyft cites to have declarations authenticating their studies. Second, Lyft's argument is founded on inadmissible hearsay. (*See* discussion, *supra*, at Section 4.2.2. of this *Ruling*.)

In addition to the foundational and hearsay problems attendant to the studies that Lyft proffered, Lyft has not carried its burden of proof because the arguments regarding harm to Lyft's passengers if trip data were released are speculative at best. That is why this *Ruling* italicized the words "might" and "impossible to anticipate" in Lyft's *Motion*—-they underscore the speculative nature of the harm that Lyft claims might befall passengers who avail themselves

[54] Lyft *Motion*, at 29.

[55] *Id.*, at 27-30.

of the Lyft app for transportation and if their trip data is disclosed. Put another way, Lyft has failed to present *any* admissible evidence that the public interest favoring nondisclosure greatly outweighs the public interest favoring disclosure.

The Commission is on solid legal ground in rejecting Lyft's request to keep trip data confidential. In *Humane Society*, the Court cautioned against accepting as true unsubstantiated invasion of privacy claims as a basis for invoking Government Code § 6255(a):

> HSUS relies on an Attorney General opinion (81 Ops.Cal.Atty.Gen. 383 (1998)) that says speculation is not a basis for denying disclosure. As reflected in that opinion, the Attorney General was asked whether senior citizens' claims for parcel tax exemptions levied by a school district are subject to public inspection. Balancing the interests, the Attorney General concluded that the claims must be disclosed. Regarding the interests on the nondisclosure side of the balance, the Attorney General observed, "if the information in question is not disclosed, the rights of privacy of the senior citizens in the district would be protected. Arguably, they would not be subject to unwanted solicitations directed to them due solely to their having surpassed the age of 65. Such speculation, however, is not a basis for denying disclosure under the terms of Section 6255." (81 Ops.Cal.Atty.Gen., *supra,* at p. 387.) Thus, the privacy concern noted by the Attorney General was nothing more than an unsubstantiated fear, not supported by evidence.[56]

Other decisions have also rejected catch-all exemption claims based on speculative assertions of privacy invasions. For example, in *CBS v. Block* (1986) 42 Cal.3d 646, 652, Defendants contend that they met the burden of proving that the records of applications and licenses for concealed weapons fall within the catch-all exception by arguing that releasing this information will allow

[56] 214 Cal.App.4th, at 1257.

would-be attackers to more carefully plan their crime against licensees and will deter those who need a license from making an application. In rejecting Defendants' argument, the Court cautioned against the reliance on speculative assertions:

> Defendants' concern that the release of the information to the press would increase the vulnerability of licensees is conjectural at best. The prospect that somehow this information in the hands of the press will increase the danger to some licensees cannot alone support a finding in favor of non-disclosure as to all. A mere assertion of possible endangerment does not "clearly outweigh" the public interest in access to these records."

(*See*, *also*, *New York Times Co. v. Superior Court* (1990) 218 Cal.App.3d 1579, 1581, 1586 [The Court held that the catchall exemption did not apply to a request for the names and addresses of water customers who exceeded their water rationing allocation. The water district had asserted that publication of the names "could expose" the individuals to verbal or physical harassment, but the Court reasoned that "the record contains no evidence that revelation of names and addresses of those who have exceeded their water allocation during a billing period will subject those individuals to infamy, opprobrium, or physical assault."]; and *California State University, Fresno Association, Inc. v. Superior Court* (2001) 90 Cal.App.4th 810, 835 [the Court compelled the University to disclose documents containing the identities of donors who, upon making donations to a university-affiliated foundation, obtained licenses to use luxury suites in a new campus arena. The Court reasoned that the University's arguments for nondisclosure were speculative and not supported by competent evidence: "[A]ny claims by the University that donations will be canceled are speculative, supported only by inadmissible hearsay. Statements by University personnel

that disclosure of the licensees will likely' have a chilling effect on future donations, resulting in a potential loss of donations, are inadequate to demonstrate any significant public interest in nondisclosure."].)

This Ruling considers the foregoing authorities instructive. The "likely" claim that *California State University* rejected as legally insufficient is synonymous to Lyft's claims of privacy invasion that are couched around the word "might." In both *California State University* and here, the claims are speculative and supported only by inadmissible hearsay. Similarly, *CBS*' and *New York Times'* rejection of the applicability of the catch-all exception based on the claim of "possible endangerment" and "could expose," respectively, is the equivalent of Lyft's use of the phrase "potentially revealing intimate personal details[.]"[57] In sum, based on the review of the evidentiary record, this *Ruling* concludes that Lyft has failed to carry its burden of proving that the public interest from nondisclosure of the trip data greatly outweighs the public interest from disclosure of the trip data.

- Uber

This *Ruling* next considers Uber's *Motion*. Uber identifies the following categories of information where it claims the public interest served by not disclosing them clearly outweighs the public interest served by disclosure: (1) confidential complaints, which Uber defines as sensitive information regarding confidential reports of harassment, assault, or other complaints; (2) driver discipline; and (3) unknowability of potentially confidential information.[58]

[57] Lyft *Motion*, at 27.

[58] Uber *Motion*, at 29-31.

As for what Uber terms confidential complaints, this *Ruling* has already made a determination that information regarding sexual assaults and sexual harassment complaints, including latitude and longitude, and settlement information, may be redacted from the public version of a TNC's Annual Report.[59] As for "other complaints," that category is too vague for this Ruling to determine if Uber has carried its burden of proof. Thus, this *Ruling* will not invoke Government Code § 6255(a) any more than it already has.

As for driver discipline information, Uber claims that the disclosure of this number "is likely to leave the public with the mistaken impression that one TNC has drivers who are more likely to commit violations than its competitor whose disciplinary standards are more lax."[60] This *Ruling* rejects Uber's concern because it is vague and unsubstantiated.

Finally, as for the "unknowability of potentially confidential information," this *Ruling* rejects this category as it is vague and unsubstantiated. Uber claims that including information regarding pending complaints potentially risks disclosing confidential information because "it is impossible for a TNC to know whether pending complaints, unresolved or otherwise pending at the time of the filing of this motion or the Annual Report, will resolve in a similar manner."[61] Yet Uber's argument undermines its request to keep complaint information confidential. At the time the complaint is made, there is no entitlement to confidentiality and Uber fails to cite to any authority. The fact that a complaint may settled confidentially in the future does not lead to the conclusion that the complaint must be treated confidentially at present.

---

[59] *Ruling*, at Section 1; and *2020 Confidentiality Ruling*, at 9-10.

[60] Uber *Motion*, at 30-31.

[61] *Id.*, at 31.

- Nomad

Nomad asserts that the following interests weigh in favor of not disclosing trip data: (1) protecting the privacy of the users of regulated platforms and services; and (2) promoting competition. This *Ruling* rejects Nomad's arguments. With respect to privacy, Nomad cites to the *Patel* decision which, as was explained above, is factually distinguishable from the instant proceeding and, therefore, cannot be relied upon to cloak trip data in a privacy blanket.[62] Next, Nomad claims that the Commission has recognized that privacy is a compelling basis for not making certain information public.[63] While true, Nomad does not cite any Commission decisions that have found that trip data as a whole is entitled to privacy protection with the exception for the limited categories of trip data information identified above.

Nomad's argument that promoting competition is a sufficiently compelling interest that would justify the nondisclosure of the trip data is also unfounded.[64] Nomad claims that the disclosure of its trip data could lead to the reverse engineering and expropriation of Nomad's trade secrets, but this *Ruling* has already rejected the trade secret claims so there is nothing in the record to support the claim that releasing trip data will stifle competition in the California TNC industry.

- HopSkipDrive

HopSkipDrive asserts three arguments to satisfy the balancing test in its favor: first, it is a small TNC focused on service public agencies who arrange rides for students, foster youth, and homeless youths, as well as elderly riders

[62] Nomad *Motion*, at 14.

[63] *Id*.

[64] Id., at 15.

and other persons who need more support, and there is a public interest in maintaining the privacy of these riders.[65] But the Annual Reports do not require the disclosure of the names of HopSkipDrive's customer base or other service public agencies who arrange for the rides so the disclosure of trip data will not invade rider privacy.

Second, because it offers a niche service, there won't be the same interest in examining whether HopSkipDrive's trip data will be useful to developing public policy programs that might reduce traffic congestion and GHG emissions.[66] While its operation may be small compared to Uber and Lyft, the fact remains that HopSkipDrive is putting vehicles on the road to further its customer's transportation interests. HopSkipDrive's trip data, even though it may be small than Uber and Lyft's trip data, nonetheless provides interested government entities with the best overall illustration of the number of TNC passenger rides are being provided by the TNC industry as a whole.

Third, HopSkipDrive claims there could be anticompetitive effects from releasing its trip data.[67] But HopSkipDrive's argument is sheer speculation. It fails to identify any competitors for the customer base it services, nor does it demonstrate that an unknown competitor could use the trip data to identify any specific customers.

On the whole, Moving Parties have failed to carry their burden of proof under Government Code § 6255(a)'s balancing test.

---

[65] HopSkipDrive *Motion*, at 8-9.

[66] *Id.*, at 9.

[67] *Id.*

4.2.2.2. Does the Public Interest in Disclosure of Trip Data Greatly Outweigh NonDisclosure?

But having found that the Moving Parties have failed to demonstrate that the public interest in nondisclosure is greater than the public interest in disclosure does not end our inquiry. This *Ruling* must also consider whether the public's interest in disclosure of TNC trip data greatly outweighs nondisclosure. In *International Federation of Professional Technical Engineers v. Superior Court* (2007) 42 Cal.4th 319, 328-329, the California Supreme Court spoke to the essential value of an open government, which includes access to government records:

> Openness in government is essential to the functioning of a democracy. "Implicit in the democratic process is the notion that government should be accountable for its actions. In order to verify accountability, individuals must have access to government files. Such access permits checks against the arbitrary exercise of official power and secrecy in the political process….
>
> As the result of an initiative adopted by the voters in 2004, this principle is now enshrined in the state Constitution: "The people have the right of access to information concerning the conduct of the people's business, and therefore, . . . the writings of public officials and agencies shall be open to public scrutiny." (Cal. Const., art. I, § 3, subd. (b)(1).)

In the case of the Commission, regulatory transparency is essential to the public's understanding how the Commission performs its responsibility of regulating entities under its jurisdiction. Additionally, transparency instills confidence in the public that the Commission is ensuring that entities under the Commission's control are providing services to Californians in a safe, reliable, and nondiscriminatory manner.

When faced with a claim that the catch-all exemption prevents the disclosure of documents in the government's possession, *Humane Society* teaches us on how to balance the two conflicting interests:

> If the records sought pertain to the conduct of the people's business there *is* a public interest in disclosure. The *weight* of that interest is proportionate to the gravity of the governmental tasks sought to be illuminated and the directness with which the disclosure will serve to illuminate.' (*Citizens for a Better Environment v. Department of Food & Agriculture* (1985) 171 Cal.App.3d 704, 715 [217 Cal.Rptr. 504], italics added.) The existence and weight of this public interest are conclusions derived from the nature of the information." (*Connell v. Superior Court* (1997) 56 Cal.App.4th 601, 616 [65 Cal.Rptr.2d 738] (*Connell*); accord, *County of Santa Clara, supra,* 170 Cal.App.4th at p. 1324.)
>
> As the court put it in *County of Santa Clara* and *City of San Jose,* "the issue is `whether disclosure would contribute significantly to public understanding of government activities.'"

Thus, in assigning *weight* to the general public's interest in disclosure, courts should look to the "nature of the information" and how disclosure of that information contributes to the public's understanding of how the government functions, and if that functioning is in the best interests of Californians.

- The nature of the information and how it is used

The trip data that the Commission has ordered each TNC to submit in its Annual Report provides the Commission, the agency tasked with regulatory oversight over TNC, with the most comprehensive account of each TNC's transportation for the past 11 months. With the trip data, the Commission can learn the number of rides each TNC provides, learn about driving patterns by examining the areas where rides commence and end, learn about the times of the day and days of the week where TNC passenger requests are highest, learn

about TNC requests accepted by geographic locations, and total amounts paid for the rides completed.

- The benefits and the public's understanding of government

The Commission's analysis and understanding of TNC trip data will enable the Commission to achieve several important objectives that are in the public interest. First, the trip data will enable the Commission to determine the safety of TNC operations and if any adjustments in the Commission's regulations should be implemented. As the Commission found in D.13-09-045:

> The Commission opened this proceeding to protect public safety and secondarily encourage innovators to use technology to improve the lives of Californians. The Commission has a responsibility for determining whether and how public safety might be affected by these TNCs. In opening this Rulemaking, the Commission wanted to assess public safety risks, and to ensure that the safety of the public is not compromised in the operation of TNCs.

With trip data as a guide, the Commission can investigate if there are any safety issues concerning the providing of TNC transportation, and if those safety issues are located in particular areas or times of day in which the service is being provided. Unquestionably, the public has an interest in seeing that the Commission satisfies its obligation to ensure that TNC drivers are operating safely.

Second, the trip data can shed light on whether TNCs are offering their service in a nondiscriminatory manner. Transportation is more than a public convenience. As the Comments from the Center for Accessible Technology point out, transportation, and the equal access to same, has become a civil rights priority:

> Transportation equity is a civil and human rights priority. Access to affordable and reliable transportation widens

> opportunity and is essential to addressing poverty, unemployment, and other equal opportunity goals such as access to good schools and health care services. However, current transportation spending programs do not equally benefit all communities and populations. And the negative effects of some transportation decisions—such as the disruption of low-income neighborhoods—are broadly felt and have long-lasting effects. Providing equal access to transportation means providing all individuals living in the United States with an equal opportunity to succeed.[68]

As a result for the need to treat all California residents equally, the Legislature enacted Civil Code § 51(b) to protects all California residents against discrimination:

> (b) All persons within the jurisdiction of this state are free and equal, and no matter what their sex, race, color, religion, ancestry, national origin, disability, medical condition, genetic information, marital status, sexual orientation, citizenship, primary language, or immigration status are entitled to the full and equal accommodations, advantages, facilities, privileges, or services in all business establishments of every kind whatsoever.

The Commission can use the trip data to ensure that all geographic locations, regardless of their economic or racial makeup, are provided with equal access to TNC services. If trip patterns reveal that some geographic locations receive greater access than others, the Commission can use the trip data to investigate those disparities and take the appropriate corrective or enforcement measures, thus assuring the public that the Commission is ensuring that TNCs do not discriminate against any class of persons.

[68] Center For Accessible Technology's *Opening Comments on OIR*, at 3-4, quoting from Leadership Conference on Civil and Human Rights website.

The public interest in ensuring the release of information to validate that industry services regulated by the state are being provided in a nondiscriminatory manner is so strong that it can overcome claims that the information is protected by trade secrets. The California Supreme Court recognized this interest in the context of insurance rates in *State Farm Mutual Automobile Insurance Company v. Garamendi* (2004) 32 Cal.4th 1029, 1047:

> Finally, the fact that insurers may invoke the trade secret privilege in the public hearing process established by Proposition 103, pursuant to Insurance Code Section 1861.08, does not dictate a different result. There is nothing anomalous about precluding insurers from invoking the trade secret privilege after they have already submitted trade secret information to the Commissioner pursuant to a regulation validly enacted under article 10 (*see ante*, at 1045), while permitting them to invoke the privilege in response to a request for information in a public rate hearing. Insurance Code Section 1861.07 merely requires public disclosure of "information provided to the commissioner pursuant to" article 10. By definition, this information is relevant to the Commissioner's mandate under article 10 to "`ensure that insurance is fair, available, and affordable for all Californians.'" (Historical and Statutory Notes, 42A West's Ann. Ins. Code, *supra*, foll. § 1861.01 at 649.) Given that article 10 seeks to encourage public participation in the rate-setting process (*see ante*, at 1045), precluding insurers from withholding trade secret information already provided to the Commissioner because of its relevance under article 10 (*see ante*, at 1040-1042) is certainly reasonable.

As the public's interest in TNC rides being offered in a nondiscriminatory manner is undoubtably as strong as the public's interest in ensuring that insurance is fair, available, and affordable, making trip data public serves a public interest that should be given great weight in the Commission's calculus.

Third, akin to the public interest in ensuring TNC rides are provided in a nondiscriminatory manner is the public interest that persons with disabilities have equal access to TNC rides. Civil Code § 54.1 specifically prohibits discrimination against persons with disabilities in the provision of services, including transportation services:

> (a)(1) Individuals with disabilities shall be entitled to full and equal access, as other members of the general public, to accommodations, advantages, facilities, medical facilities, including hospitals, clinics, and physicians' offices, and privileges of all common carriers, airplanes, motor vehicles, railroad trains, motorbuses, streetcars, boats, or any other public conveyances or modes of transportation (whether private, public, franchised, licensed, contracted, or otherwise provided), telephone facilities, adoption agencies, private schools, hotels, lodging places, places of public accommodation, amusement, or resort, and other places to which the general public is invited, subject only to the conditions and limitations established by law, or state or federal regulation, and applicable alike to all persons.

Similarly, on the federal level, Title II of the Americans with Disabilities Act prohibits disability-based discrimination in providing public and private services.[69] Public and or private entities that provide transportation services to the public are required by law to be accessible to individuals with disabilities.

[69] 28 CFR 35.130 General prohibitions against discrimination

a. No qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of a public entity, or be subjected to discrimination by any public entity.

Under the Americans with Disabilities Act (ADA), TNCs are considered private entities primarily engaged in transportation and are required to be accessible to individuals with disabilities.[70]

California recognized the importance of providing TNC service access to persons with disabilities when it amended Pub. Util. Code §5440 as follows:

> (f) There exists a lack of wheelchair accessible vehicles (WAVs) available via TNC online-enabled applications or platforms throughout California. In comparison to standard vehicles available via TNC technology applications, WAVs have higher purchase prices, higher operating and maintenance costs higher fuel costs, and higher liability insurance, and require additional time to serve rider who use nonfolding motorized wheelchairs.
>
> (g) It is the intent of the Legislature that California be a national leader in the deployment and adoption of on-demand transportation options for persons with disabilities.

Trip data can provide the initial understanding into whether persons with disabilities are given fair and equal access to TNC rides. In addition to the applicability of ADA protections to TNCs, in September 2018, the Governor signed into state law Senate Bill (SB) 1376: TNC Access for All Act (Hill, 2018). Pursuant to SB 1376, the Commission must establish a program relating to accessibility for persons with disabilities as part of its regulation of TNCs. While implementation of SB 1376 is occurring in Rulemaking 19-02-012, the trip data developed and submitted in this proceeding can assist the Commission develop

[70] Private entities that are primarily engaged in the business of transporting people and whose operations affect commerce shall not discriminate against any individual on the basis of disability in the full and equal enjoyment of specified transportation services. This obligation includes, with respect to the provision of transportation services, compliance with the requirements of the rules of the Department of Justice concerning eligibility criteria, making reasonable modifications, providing auxiliary aids and services, and removing barriers (28 CFR 36.301-36.306).

regulations specific to persons in wheelchairs to help these persons have access to TNC rides.

Fourth, the trip data can help the public understand the impact of TNC vehicles on traffic congestion, infrastructure, and airborne pollutants. With Government Code § 65088, the Legislature made the following findings regarding the need to alleviate traffic congestion and air pollution:

a. Although California's economy is critically dependent upon transportation, its current transportation system relies primarily upon a street and highway system designed to accommodate far fewer vehicles than are currently using the system.
b. California's transportation system is characterized by fragmented planning, both among jurisdictions involved and among the means of available transport.
c. The lack of an integrated system and the increase in the number of vehicles are causing traffic congestion that each day results in 400,000 hours lost in traffic, 200 tons of pollutants released into the air we breathe, and three million one hundred thousand dollars ($3,100,000) added costs to the motoring public.
d. To keep California moving, all methods and means of transport between major destinations must be coordinated to connect our vital economic and population centers.
e. In order to develop the California economy to its full potential, it is intended that federal, state, and local agencies join with transit districts, business, private and environmental interests to develop and implement comprehensive strategies needed to develop appropriate responses to transportation needs.

The public has an interest in the Commission sharing trip data with government entities responsible for addressing transportation issues such as congestion, air pollution, and impact on infrastructure. The trip data can show the number

of TNC vehicles in service on a given date and time, where the vehicles are concentrated, the overall impact on traffic congestion, impact on road usage, and the impact TNC vehicles have on other service vehicles (*e.g.* public buses, private shuttles, taxis, and vans) that share the same roads.

Thus, when the Commission applies the balancing test to determine the applicability, if any, of the catch-all exemption to Moving Parties' trip data, this *Ruling* concludes that the public interest in disclosing TNC trip data far outweighs the benefits from not disclosing TNC trip data.

5. Moving Parties Have Failed to Meet Their Burden of Proving that the Trip Data is Protected from Public Disclosure on Privacy Grounds

5.1. Government Code § 6254(c)

The foundation for Moving Parties' claim of trip data privacy is Government Code § 6254(c) which provides an exemption in the CPRA for "personnel, medical, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy."[71] While the statute does not define "privacy" the California Supreme Court offered the following guidance in *International Federation of Professional and Technical Engineers v. Superior Court* (2007) 42 Cal.4th 319, 330: "'A particular class of information is private when well-established social norms recognize the need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity." (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 35.'" In

[71] Lyft *Motion*, at 15, and 26-32. Both Nomad and HopSkipDrive agree with the factual and legal contentions that Lyft and Uber have made for the 2020 and 2021 Annual Reports, so by extension they are also relying on Government Code § 6254(c). (*See* Nomad *Motion*, at 5; HopSkipDrive *Motion*, at 5.)

Hill, the California Supreme Court established a three-part test for determining the legitimacy of an invasion of privacy claim: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct that constitutes a serious invasion of privacy.[72]

Even if the three-part test is met, *Hill* notes that an "invasion of a privacy interest is not a violation of the state constitutional right to privacy" *per se*.[73] Instead, when a claim of privacy is made, *Williams v. Superior Court* (2017) 3 Cal.5th 531, 556, instructs that there must be a consideration of the seriousness of the privacy claim to determine what competing interest must be shown for the information's disclosure:

> Not every assertion of a privacy interest under article I, Section 1 must be overcome by a compelling interest. Neither the language nor history of the Privacy Initiative unambiguously supports such a standard. In view of the far-reaching and multifaceted character of the right to privacy, such a standard imports an impermissible inflexibility into the process of constitutional adjudication. (citation omitted). A compelling interest is still required to justify an obviously invasion of an interest fundamental to personal autonomy. (citation omitted.) But whenever lesser interests are at stake, the more nuanced framework discussed above applies, with the strength of the countervailing interest sufficient to warrant disclosure of private information varying according to the strength of the privacy interest itself, the seriousness of the invasion, and the availability of alternatives and protective measures.

Thus, the seriousness of the privacy claim turns on whether there is an effort to obtain data that would come under the category of informational privacy versus

[72] 7 Cal.4th, 39-40.

[73] 7 Cal.4th, 38.

autonomy privacy. When a claim of informational privacy is made and the three-part test articulated in *Hill* is met, the party seeking the information needs to establish a legitimate and important interest in the disclosure.[74] In *Hill*, the California Supreme Court explained that interest as follows:

> legitimate interests derive from the legally authorized and socially beneficial activities of government and private entities. Their relative importance is determined by their proximity to the central functions of a particular public or private enterprise.[75]

In contrast, when the request seeks more sensitive personal information such as medical or financial details or personal autonomy, the requesting party's interest in the information must be compelling. The *Williams* decision put name and contact information in the informational privacy category such that only a legitimate and important interest, rather than a compelling need for the information, need be shown. While the foregoing legal discussion in *Hill* arose in the context of the NCAA's ability to collect samples from college athletes to perform drug tests, and Williams involved the right to discovery, this *Ruling* finds that the California Supreme Court's decisions are also instructive in resolving Moving Parties' claim that the government's proposed release of trip data would be an impermissible invasion of privacy.

- Does Trip Data Include a Legally Protected Privacy Interest?

The first inquiry is whether Moving Parties demonstrate that the trip data at issue fits within *Hill's* three-part test for privacy, and this *Ruling* answers that question in the negative. With the elimination of the presumption of

[74] 3 Cal.5th, 552-554.

[75] 7 Cal.4th, 38.

confidentiality attendant to the Annual Reports, a claim of confidentiality based on privacy, or any other legally recognized grounds, must be affirmatively established. The *2020 Confidentiality Ruling* determined that the bulk of trip data categories required by the 2020 Annual Reports were not privacy protected and Moving Parties have failed to set forth a credible factual and legal argument that would require a different finding for the 20201 Annual Reports. While Courts have deemed home contact information to be private,[76] the trip data itself does not ask for contact information. Moving Parties appear to agree that individual trip data categories do not invade protected privacy and, instead, argue that trip data can be manipulated through a re-identification process that can lead to the revelation of contact information. By their own argument, Moving Parties must acknowledge that trip data does not reveal information about a rider or driver that would rise to a constitutionally protected privacy right.

But as Moving Parties have spent a considerable amount of time on their data re-identification argument, this *Ruling* will explain why the argument fails to establish that trip data can lead to the discovery of private information. Lyft claims that the granular trip data can be manipulated to identify specific individuals and track their movements, "potentially revealing intimate personal details, such as medical visits, political affiliations, personal relationships, sexual orientation, etc."[77] To establish this claim, Lyft first references the United States Census Bureau documents that are attached to its *Motion* as Exhibit A and argues that because some census blocks may include as few as five individuals, and 4,000,000 census blocks in the United States have zero population, there are

[76] *Williams*, *supra*, 3 Cal.5th, 554

[77] Lyft *Motion*, at 27.

privacy implications from producing trip data census block information.[78] Yet Lyft does not claim that any of its TNC drivers travel from or to census blocks with few to no individuals, and that those trips are part of the information provided to the Commission in Lyft's 2021 Annual Report.

This *Ruling* also faults Lyft for attempting to rely on a Census Bureau 2020 Disclosure Avoidance Modernization project, as well as comments from the Director of the Federal Trade Commission's Bureau of Consumer Protection, because they are inadmissible hearsay.[79] While Section 4.2.2. of this *Ruling* set out in detail the hearsay rule and how, under appropriate circumstances, hearsay can be admitted into evidence before the Commission, Lyft has not attempted to meet that requisite showing. Lyft has not submitted any declaration from the US Census Bureau or the Federal Trade Commission, nor has Lyft submitted a request for official notice, so this *Ruling* will not accept as true any statements or conclusions from the project or the testimony.[80]

---

[78] *Motion*, at 28.

[79] *Id*., and at 29.

[80] Even if Lyft had asked the Commission to take official notice of the Census Bureau project of the Director of the Federal Trade Commission's Bureau of Consumer Protection testimony report pursuant to Rule 13.10, such an effort would not have advanced Lyft's cause. If the Commission had taken official notice of the project and testimony it would not have taken official notice of the findings and conclusions as to whether trip data can be engineered to (1) reveal a passenger's identity; (2) reveal the starting and ending addresses of a TNC trip; and (3) reveal a driver's identity, because these findings and conclusions are reasonably subject to dispute and, therefore, may not necessarily be correct. (*See Apple Inc. v. Superior Court* (2017) 18 Cal.App.5th 222, 241 ["judicial notice of a document does not extend to the truthfulness of its contents or the interpretation of statements contained therein, if those matters are reasonably disputable."] Numerous other decisions are in accord with this limitation on the use of judicial notice. (*See Richtek USA, Inc. v. UPI Semiconductor* (2015) 242 Cal.App.4th 651, 660-662 [facts in pleadings]; *Kilroy v. State of California* (2004) 119 Cal.App.4th 140, 148 [findings of fact in prior judicial opinion]; *Lockley v. Law Office of Cantrell, Green Pekich, Cruz & McCort* (2001) 91 Cal.App.4th 875, 882 [hearsay statements in decisions and court files]; and *Sosinsky v. Grant* (1992) 6 Cal.App.4th 1548, 1565 and 1568 [truth of judge's factual finding.) This reluctance also

Footnote continued on next page.

Lyft next refers to a series of opinions to support its claim that disclosed trip data can lead to an invasion of rider privacy by way of information re-identification. Lyft references a study involving the inadvertent release of New York City taxi data, and to a paper entitled *The Tradeoff between the Utility and Risk of Location Data and Implications for Public Good* that allegedly found that geolocation data aggregated to the census block level presents "a series risk of de-identification."[81] Finally, Lyft cites to Health Insurance portability and Accountability Act rules that data linked to zip codes with fewer than 20,000 residents, medical data can be re-identified.[82] This *Ruling* declines to consider the testimony, paper, and rules in that they are all inadmissible hearsay. Lyft does not explain why it 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*.[83] This *Ruling* rejects and will not consider this information as it is inadmissible hearsay.

Nor is Lyft's position supported by the Rosenthal Declaration. With respect to the invasion of privacy claim, he states:

> Because the public disclosure of the Census Block Trip Data may allow third parties to identify particular individuals and track their movements, potentially exposing them to danger,

---

extends to not taking official notice of the truth of allegations in affidavits, declarations, and reports. (*See Bach v. McNelis* (1989) 207 Cal.App.3d 852, 865 [affidavits]; Tarr v. Merco Construction Engineers, Inc. (1978) 84 Cal.App.3d 707, 715 [affidavits, pleadings, and allegations]; and *Ramsden v. Western Union* (1977) 71 Cal.App.3d 873, 878-879 [arrest report].)

[81] Lyft *Motion*, at 29-31.

[82] *Id.*, at 32.

[83] This *Ruling* also declines to consider the other studies (an MIT study, cited on page 31 of Lyft's *Motion*) and articles (cited in footnotes 92-95, and 98-99) that Lyft has cited as they are inadmissible hearsay.

> embarrassment, ridicule, or liability, the data is protected from disclosure pursuant to Government Code § 6254(c) as a file the disclosure of which would constitute an un unwarranted invasion of privacy, and § 6254(k) and the Right of Privacy guaranteed by Article I, Sect.1, of the California Constitution.[84]

There are several legal infirmities with this Declaration. First, it is not based on person knowledge. Second, with the use of the words "may" and "potentially," the claims made therein are speculative. Third, it contains legal conclusions which are inappropriate for a declaration.[85] As such, the Rosenthal Declaration will not be given any weight on the privacy issue.

The showings by the other Moving Parties are equally deficient when it comes to establishing a privacy claim for trip data. Uber relies on a series of studies and claims it employed Privacy Analytics, Inc. to review the re-identification risk associated with the sharing of trip data from the Annual Report.[86] This *Ruling* will not consider these reports and the work by Privacy Analytics, Inc. as they are all inadmissible hearsay. Additionally, the Sivram Declaration lacks personal knowledge to support Uber's privacy assertions. Instead, in paragraphs 4-8, the Sivram Declaration refers to the work performed by Privacy Analytics, Inc. In paragraph 9, the Sivram Declaration prefaces the claims with the phrase "applying this research with my knowledge

---

[84] Rosenthal Decl., ¶ 12.

[85] *See Jack v. Wood* (1968) 258 Cal.App.2d 639, 645: "Legal conclusions are especially objectionable when they are contained in the moving party's affidavits. *(Gardenswartz v. Equitable etc. Soc.*, 23 Cal. App. 2d Supp. 745, 753-754 [68 P.2d 322]; *Low v. Woodward Oil Co., Ltd.*, 133 Cal. App. 2d 116, 121 [283 P.2d 720]; *Weichman v. Vetri*, 100 Cal. App. 2d 177, 179 [223 P.2d 288]; *Fidelity Investors, Inc. v. Better Bathrooms, Inc.*, 146 Cal. App. 2d Supp. 896 [304 P.2d 283].)"

[86] Uber Motion, at 6-10, and 15-17; and Declaration of Uttara Sivram, ¶¶ 4-8, and Exhibit 1 thereto.

of the technical practicalities associated with trip data[.]" But as the declarant is referencing the Privacy Analytics, Inc. work again, the value of paragraph 9 is discounted.

Moreover, the Sivram Declaration does not say what the declarant's knowledge is of the "technical practicalities associated with trip data." While the declarant claims to be Uber's Head of Public Policy for Privacy and Security," that title, without more, is insufficient to establish that the declarant has the necessary personal knowledge to support the assertions therein. Furthermore, the declarant's conclusions in paragraph 9 are also based on a concept called "k-anonymity," which the declarant learned of by referencing and using something called the "Open Data Release Toolkit from DataSF, the International Organization for Standardization's privacy standard on enhancing data de-identification terminology and classification of techniques, as well as other scholarly sources." This *Ruling* will not rely on the statements contained in paragraph 9 because they are based on multiple sources of inadmissible hearsay.[87]

Nomad's argument for privacy of trip data is equally unpersuasive. While Nomad cites to Government Code § 6254(c), it does not set forth its own argument.[88] Instead, Nomad agrees with and relies on the "factual and legal contentions made by Uber and Lyft in 2020 and 2021 regarding

[87] Since this *Ruling* has declined to consider paragraphs 4-9 of the Sivaram Declaration, we need not consider if the information claimed in paragraph 10 of the Sivaram Declaration presents a reasonable alternative to ensure the geographical units and time periods included per trip record are wide enough to encompass a reasonably large number of trips.

[88] Nomad *Motion*, at 5.

confidentiality[.]"[89] As such, Nomad's claim for privacy of the trip data must also be rejected as unproven.

That conclusion is not altered by the Golde Declaration that Nomad provided because the declarant's concern over re-identification and loss of privacy are speculative. (*See* Golde Decl., ¶ 11 in which declarant claims because of Nomad's small scale of service "it *could be possible* to re-identify a driver partner on the basis of other quasi-identifiers even if a driver partner's unique identification number or vehicle identification number are both omitted from disclosure.") (Italics added.)

In sum, this *Ruling* finds that Moving Parties have failed to establish that trip data is a legally protected privacy interest.

- Reasonable Expectation of Privacy

Because Moving Parties have failed to establish that trip data should be protected from disclosure on privacy grounds, they cannot meet the reasonable expectation of privacy criterion. Additionally, Moving Parties fail to cite any provision in their service agreements that trip data will be treated confidentially, or that passengers are allowing the TNCs to collect the trip data with the understanding that it will be kept private.

- Harm from serious invasion

Finally, Moving Parties fail to establish that the disclosure of the trip data would be a serious invasion of privacy. As noted above, the claims that the trip data can be reidentified to reveal personal information about a rider's politics, religious beliefs, sexual orientation, or medical status are speculative and based on inadmissible evidence.

[89] *Id*.

In addition, this *Ruling* rejects Uber's further claim about the harm from the release of trip data as it, too, is speculative. Paragraph 11 of the Sivaram Declaration claims that keeping trip data confidential could limit the number of individuals "who could perform re-identification with the dataset," and releasing the data to the public leaves open the possibility of any member of the public, including a motived adversary, "to access the data for re-identification purposes. The use of the words "might," "possibility," and the unidentified "motivated adversary" only serve to underscore the speculative nature of the harm Uber claims will occur if trip data is released to the public. Such speculation and lack of personal knowledge are insufficient to establish a privacy claim for the trip data.

- Personal Autonomy versus Informational Privacy

Even if *Hill's* three-part test had been met, this *Ruling* must next address if trip data falls into the personal autonomy category, where a compelling interest must be shown for its disclosure (collection), or the informational privacy category, where there only needs to be a legitimate and important interest in its disclosure. As trip data does not fall within the personal autonomy category, which deals with a person's medical records or personnel file, trip data would fall within the informational privacy category where a less stringent standard is employed to determine if the information should be released to the public.

Initially, this *Ruling* concludes that the Commission satisfies the lesser legitimate and important interest standard. Gathering trip data is part of the Commission's duty to regulate and understand all facets of each TNC's passenger services. Both the California Constitution and the Public Utilities Code vest the Commission with expansive authority to investigate TNCs companies, which would include learning about rides provided and using that

information to promulgate any additional regulations and reporting requirements regarding TNC passenger services.

This *Ruling* is unaware of any law that would require the Commission to satisfy a heightened preliminary proof requirement to obtain information regarding trip data. In *Williams*, the California Supreme Court rejected the imposition of a heightened preliminary showing as none was required by the statute: "If the Legislature intended to demand more than mere allegations as a condition to the filing of suit or preliminary discovery, it could have specified as much. That it did not implies no such heightened requirement was intended."[90] *Williams* went further and cautioned that to insert such a requirement would "undercut the clear legislative purposes the act was designed to serve."[91] Similarly, to impose a heightened proof requirement on the Commission when none appears within the Public Utilities Code would frustrate the Commission's ability to carry out the will of the Legislature that it regulate and investigate entities subject to its jurisdiction.

Even if the Commission had to satisfy the compelling state interest standard, it can do so. The Commission is tasked by the California Constitution and the Legislature to regulate services in a manner that protects the safety of the persons who avail themselves of those services. Ensuring public safety is perhaps one of the most compelling state interests that the Commission is tasked with protecting. When that duty is combined with the Constitutional mandate to conduct governmental operations with the greatest transparency and to give the public access to government records unless prohibited by law, this *Ruling* finds

[90] 3 Cal.5th, 546.

[91] *Id*.

that there is a compelling state interest in making the trip data public even if it did have protected privacy status under *Hill*.

5.2. Family Educational Rights and Privacy Act

As a TNC specializing in the transport of minors, HopSkipDrive presents an additional argument in support of its claim for the confidential treatment of trip data. It cites to the Family Educational Rights and Privacy Act (FERPA), which is a federal law "that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education."[92] FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;

[92] 20 U.S.C. § 1232(g); 34 CFR Part 99. HopSkipDrive *Motion*, at 5; and Donahue Decl., ¶ 11.

- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

It is unclear how the trip data that HopSkipDrive provides to the Commission in its Annual Report fits within the protections provided by FERPA. There is no reportable category for school records in the data reporting templates that CPED has prepared, nor is it a reportable category in the prior Commission decisions. As such, HopSkipDrive's reliance on FERPA is misplaced.

HopSkipDrive's argument regarding trip data's disclosure of and endangering rides for youths in the foster system is also unpersuasive.[93] The Annual Report requirements do not include personal information, and HopSkipDrive fails to explain how the release of geo-location data will lead to the identification of a youth in the foster system.

5.3. Fare Factors

HopSkipDrive asks for confidential protection for fare factors on the grounds that it is protected private information.[94] This *Ruling* rejects HopSkipDrive's request as it fails to satisfy the *Hill* factors for the determining if fare information is private.

[93] HopSkipDrive *Motion*, at 7-8.

[94] *Id.*, at 12.

IT IS RULED that:

1. The *Ruling* finds that Moving Parties may redact the following information from the public versions of the 2021 Annual Reports on the grounds that the information is confidential:

- Latitude and longitude information in all data categories.
- Driver information in all data categories: drivers' names, type of driver identification, license state of issuance, license number, expiration date, description of allegation, definition, type and description of alleged sexual assault or sexual harassment, and vehicle VIN.
- Accidents and incidents: the parties involved in the incident, any party found liable in an arbitration proceeding, information concerning any criminal proceeding if the record has been sealed by the court, amounts paid by the TNC's insurance, driver's insurance, or by any other source.

2. The Ruling denies the balance of Moving Parties Motions. Appendix A to this Ruling provides a category-by-category identification, which tracks the reporting template, of what information required by the 20201 Annual Reports is confidential and what information should be made public.

3. This *Ruling* also will apply to *Motions for Confidential Treatment* that Nomad Transit and HopSkipDrive filed for their 2020 Annual Reports.

Dated November 24, 2021, at San Francisco, California.

/s/ ROBERT M. MASON III
Robert M. Mason III
Administrative Law Judge

APPEDNIX A

(2021 ANNUAL REPORT TEMPLATE)

APPENDIX A

Driver Names & IDs

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
DriverID	Confidential
DriverFirstName	Confidential
DriverMI	Confidential
DriverLastName	Confidential
DriverLicNum	Confidential
DriverLicState	Confidential
DriverLicExp	Confidential

Accessibility Report

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
Month	Public
Year	Public
NumRidesReq	Public
HrsAccessVehAvail	Public
NumAccessVeh	Public
NumAccessVehReq	Public
PercentAccessVehReq	Public
NumAccessVehFilled	Public
PercentAccessVehFilled	Public

Accessibility Complaints

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
DateDiscrim	Public
DriverID	Confidential
ServiceIssue	Public
ServiceIssueDef	Public
Resolution	Public
Comments	Public

Accidents & Incidents

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
RideID	Public
Waybill1	Public
Waybill2	Public
Waybill3	Public
Waybill4	Public
Waybill5	Public
Waybill6	Public
Waybill7	Public
ComplaintID	Public
DriverID	Confidential
VIN	Confidential
VehicleMake	Public
VehicleModel	Public
VehicleYear	Public
IncidentAccidentDate	Public
IncidentAccidentLat	Confidential
IncidentAccidentLong	Confidential
IncidentAccidentZip	Public
IncidentAccidentTract	Public
IncidentAccidentCB	Public
ComplaintFiledDate	Public
IncidentAccidentType	Public
IncidentAccidentParty	Confidential
IncidentParty1	Confidential
IncidentParty2	Confidential
IncidentParty3	Confidential
IncidentParty4	Confidential
IncidentParty5	Confidential
IncidentAccidentClaim	Public

IncidentAccidentDescr	Public
PrimaryCollisionFactor	Public
IncidentAccidentGuiltyParty	Confidential
Liability	Confidential, if the proceeding is a criminal proceeding and the record has been sealed by the court
ProceedingInProgress	Confidential, if the proceeding is a criminal proceeding and the record has been sealed by the court
CourtFileNum	Confidential, if the proceeding is a criminal proceeding and the record has been sealed by the court
ProceedingStatus	Confidential, if the proceeding is a criminal proceeding and the record has been sealed by the court
PoolTrip	Public
AmountPaidAnyParty	Confidential
AmountPaidDriverIns	Confidential
AmountPaidTNC	Confidential
AmountPaidOther	Confidential
ComplaintResolveDate	Public
AccidentPeriodWaybill1	Public
AccidentPeriodWaybill2	Public
AccidentPeriodWaybill3	Public
AccidentPeriodWaybill4	Public
AccidentPeriodWaybill5	Public
AccidentPeriodWaybill6	Public
AccidentPeriodWaybill7	Public

Assaults & Harassments

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
RideID	Public
Waybill1	Public
Waybill2	Public
Waybill3	Public
Waybill4	Public
Waybill5	Public
Waybill6	Public
Waybill7	Public
ComplaintID	Public
DriverID	Confidential
VIN	Confidential
VehicleMake	Public
VehicleModel	Public
VehicleYear	Public
AssaultHarassDate	Public
AssaultHarassLat	Confidential
AssaultHarassLong	Confidential
AssaultHarassZip	Public
AssaultHarassTract	Public
AssaultHarassCB	Public
ComplaintFiledDate	Public
Investigation	Public
DriverSuspendDate	Public
PassengerSuspendDate	Public
ComplaintResolveDate	Public
AssaultHarassType	Confidential, only for sexual assault and sexual harassment
AssaultHarassDescr	Confidential
AssaultHarassDef	Confidential, only for sexual assault and sexual harassment
PoolTrip	Public

DriverConsequence	Public
ComplaintResolveDescr	Confidential
DriverCurrentAuth	Public

50,000+ Miles

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
DriverID	Confidential
VIN	Confidential
VehicleMake	Public
VehicleModel	Public
VehicleYear	Public
LeaseOwned	Public
TotalMiles	Public

Number of Hours

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
DriverID	Confidential
DriverHoursYear	Public
DriverHoursMonth	Public
DriverHoursDay	Public
DriverHoursRecordedDay	Public

Number of Miles

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
DriverID	Confidential
DriverMilesYear	Public
DriverMilesMonth	Public
DriverMilesDay	Public
DriverMilesRecordedDay	Public

Driver Training

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
DriverTrainYear	Public
DriverTrainMth	Public
DriverTrainDay	Public
EligibleDrivers	Public

Law Enforcement Citations

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
RideID	Public
Waybill1	Public
Waybill2	Public
Waybill3	Public
Waybill4	Public
Waybill5	Public
Waybill6	Public
Waybill7	Public
CitationID	Public
DriverID	Confidential
VIN	Confidential
VehicleMake	Public
VehicleModel	Public
VehicleYear	Public
CitationOfficerFirstName	Public
CitationOfficerMI	Public
CitationOfficerLastName	Public
CitationLocation	Public
NumViolations	Public
CitationAmountInitial	Public
CitationAppeal	Public
CitationAmountFinal	Public
Payor	Public
CitationReason	Confidential

Off-platform Solicitation

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
DriverID	Confidential
VIN	Confidential
VehicleMake	Public
VehicleModel	Public
VehicleYear	Public
IncidentDate	Public
ComplaintFiledDate	Public
ComplaintResolveDate	Public
OffPlatformSolicitationLat	Confidential
OffPlatformSolicitationLong	Confidential
OffPlatformSolicitationZip	Public
OffPlatformSolicitationTract	Public
OffPlatformSolicitationCB	Public
OffPlatformSolicitationDescr	Confidential
InvestigationConducted	Public
DriverConsequence	Public
ComplaintResolvedDescr	Confidential
DriverCurrentAuth	Public

Aggregated Requests Accepted

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
ZipCodeRequest	Public
TotalAcceptedTrips	Public

Requests Accepted

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
RideID	Public
Waybill1	Public
Waybill2	Public
Waybill3	Public
Waybill4	Public
Waybill5	Public
Waybill6	Public
Waybill7	Public
DriverID	Confidential
VIN	Confidential
VehicleMake	Public
VehicleModel	Public
VehicleYear	Public
AppOnOrPassengerDroppedOffLat	Confidential
AppOnOrPassengerDroppedOffLong	Confidential
AppOnOrPassengerDroppedOffZip	Public
AppOnOrPassengerDroppedOffTract	Public
AppOnOrPassengerDroppedOffCB	Public
AppOnOrPassengerDroppedOffDate	Public
TripReqRequesterLat	Confidential
TripReqRequesterLong	Confidential
TripReqRequesterZip	Public
TripReqRequesterTract	Public
TripReqRequesterCB	Public
TripReqDriverLat	Confidential
TripReqDriverLong	Confidential
TripReqDriverZip	Public
TripReqDriverTract	Public
TripReqDriverCB	Public

TripReqDate	Public
PeriodOneMilesTraveled	Public
ReqAcceptedDate	Public
ReqAcceptedLat	Confidential
ReqAcceptedLong	Confidential
ReqAcceptedZip	Public
ReqAcceptedTract	Public
ReqAcceptedCB	Public
PassengerPickupDate	Public
PeriodTwoMilesTraveled	Public
PassengerPickupLat	Confidential
PassengerPickupLong	Confidential
PassengerPickupZip	Public
PassengerPickupTract	Public
PassengerPickupCB	Public
PassengerDropoffDate	Public
PassengerDropoffLat	Confidential
PassengerDropoffLong	Confidential
PassengerDropoffZip	Public
PassengerDropoffTract	Public
PassengerDropoffCB	Public
PeriodThreeMilesTraveled	Public
PoolRequest	Public
PoolMatch	Public
TotalAmountPaid	Public
Tip	Public
FareFactor1	Public
FareFactor2	Public
FareFactor3	Public
FareFactor4	Public
FareFactor5	Public
FareFactor6	Public
FareFactor7	Public

FareFactor8	Public
FareFactor9	Public
FareFactor10	Public
FareFactor11	Public
FareFactor12	Public
FareFactor13	Public
FareFactor14	Public
FareFactor15	Public
SurgePricing	Public
VehicleOccupancyP1	Public
VehicleOccupancyP2	Public
VehicleOccupancyP3	Public
ServiceType	Public

Requests Accepted Periods

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
Waybill	Public
DriverID	Confidential
VIN	Confidential
VehicleMake	Public
VehicleModel	Public
VehicleYear	Public
Period	Public
PeriodStartDate	Public
PeriodStartLat	Confidential
PeriodStartLong	Confidential
PeriodStartZip	Public
PeriodStartTract	Public
PeriodStartCB	Public
PeriodEndDate	Public
PeriodEndLat	Confidential
PeriodEndLong	Confidential
PeriodEndZip	Public
PeriodEndTract	Public
PeriodEndCB	Public
PeriodMilesTraveled	Public
PoolRequest	Public
PoolMatch	Public
SurgePricing	Public
ServiceType	Public

Aggregated Requests Not Accepted

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
ZipCodeRequest	Public
TotalNotAcceptedTrips	Public

Requests Not Accepted

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
DriverID	Confidential
VIN	Confidential
VehicleMake	Public
VehicleModel	Public
VehicleYear	Public
TripReqDate	Public
TripReqRequesterLat	Confidential
TripReqRequesterLong	Confidential
TripReqRequesterZip	Public
TripReqRequesterTract	Public
TripReqRequesterCB	Public
TripRequesterDestinationLat	Confidential
TripRequesterDestinationLong	Confidential
TripRequesterDestinationZip	Public
TripRequesterDestinationTract	Public
TripRequesterDestinationCB	Public
NotAcceptedDate	Public
NotAcceptedDriverLat	Confidential
NotAcceptedDriverLong	Confidential
NotAcceptedDriverZip	Public
NotAcceptedDriverTract	Public
NotAcceptedDriverCB	Public
NotAcceptedDriverReason	Public
PoolRequest	Public

Suspended Drivers

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
DriverID	Confidential
ComplaintID	Public
SuspensionDate	Public
ReactivationDate	Public
SuspensionReason	Confidential
DriverPermDeactivated	Public

Total Violations & Incidents

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
DriversNotSuspended	Public
DriversSuspended	Public
DriversCommittedViolation	Public
ViolationsIncidentsReported	Public

Zero Tolerance

Field	Confidential or Public
TNCID	Public
SubmissionDate	Public
RideID	Public
Waybill1	Public
Waybill2	Public
Waybill3	Public
Waybill4	Public
Waybill5	Public
Waybill6	Public
Waybill7	Public
ComplaintID	Public
DriverID	Confidential
VIN	Confidential
VehicleMake	Public
VehicleModel	Public
VehicleYear	Public
ZeroToleranceDate	Public
ZeroToleranceLat	Confidential
ZeroToleranceLong	Confidential
ZeroToleranceZip	Public
ZeroToleranceTract	Public
ZeroToleranceCB	Public
ComplaintFiledDate	Public
ComplaintResolveDate	Public
ZeroToleranceDescr	Confidential
PoolTrip	Public
Investigation	Public
DriverConsequence	Public
ComplaintResolveDescr	Confidential
DriverCurrentAuth	Public

(END OF APPENDIX A)