BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA

FILED
09/22/17
04:59 PM

Order Instituting Rulemaking to Improve Public Access to Public Records Pursuant to the California Public Records Act	Rulemaking 14-11-001 (filed November 6, 2014)

NOTICE OF TNC WORKING GROUP PROPOSAL FOR ADDITIONAL CONFIDENTIAL MATRICES

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

September 22, 2017

Attorneys for Lyft, Inc.

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA

Order Instituting Rulemaking to Improve Public Access to Public Records Pursuant to the California Public Records Act.	Rulemaking 14-11-001 (filed November 6, 2014)

NOTICE OF TNC WORKING GROUP PROPOSAL FOR ADDITIONAL CONFIDENTIAL MATRICES

Pursuant to the Assigned Commissioner's Ruling Regarding Phase 2B: Development Of Confidential Matrices, dated August 18, 2017 ("ACR"), the TNC Working Group, composed of Lyft, Inc. and Rasier-CA, LLC ("Rasier"),[1] hereby provide notice of their request to supplement the list of proposed matrices set forth in the ACR with additional confidential matrices that have particular relevance to the TNC industry. In particular, the TNC Working Group proposes that the Commission adopt the following confidential matrix categories:

1. Confidential/proprietary data protected from disclosure under Gov't Code §6254(k) and Evidence Code §1060 as a Trade Secret
2. Customer/user activity files protected under Gov't Code §6254(c) and §6254(k)
3. Customer/user incident reports protected under Gov't Code §6254(c) and §6255(a)
4. CPUC annual reports and related supplemental data requests submitted to the Commission under assurances of confidentiality

Below, the TNC Working Group explains its proposals for additional matrix categories and the reasons why the Commission should adopt them.

1. Confidential/proprietary TNC data protected from disclosure under Government Code §6254(k) and Evidence Code §1060 as a Trade Secret

Among the matrices listed in the ACR is a matrix category for competitive information subject to protection from disclosure under Gov't Code §6255(a). Section 6255(a), commonly referred to as the public interest balancing test, is a "catchall exception" used to protect records from disclosure that would not otherwise be protected where "on the facts of the particular case the

[1] As of this filing, no other parties have requested to join the TNC Working Group.

public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record." *International Federation of Professional and Technical Engineers, Local 21, AFL-CIO v. Superior Court*, 42 Cal. 4th 319, 329 (2007). As the ACR indicates, the §6255(a) "public interest" balancing test can be appropriately employed to protect competitive information of a regulated entity from disclosure. This is because there is a strong public interest in encouraging vigorous competition for the benefit of consumers. *See Morlife, Inc. v. Perry,* 56 Cal.App.4th 1514, 1520 (1997) ("Yet also fundamental to the preservation of our free market economic system is the concomitant right to have the ingenuity and industry one invests in the success of the business or occupation protected from the gratuitous use of that "sweat-of-the-brow" by others."); *United States v. Tribune Publishing Company* (C.D. Cal., Mar. 18, 2016, No. CV1601822ABPJWX) 2016 WL 2989488, at *5 ("[T]he preservation of competition is always in the public interest."); *United States v. Columbia Pictures Indus., Inc.*, 507 F. Supp. 412, 434 (S.D.N.Y. 1980) ("Far more important than the interests of either the defendants or the existing industry... is the public's interest … in the preservation of competition."). Thus, the TNC Working Group supports the development of such a matrix for competitive information that is not otherwise protected from disclosure under the Public Records Act.

The TNC Working Group also notes, however, that much of the competitively sensitive information maintained by TNCs is independently protected from disclosure as trade secret information pursuant to Gov't Code § 6254(k) and Evidence Code §1060. Section 6254(k) exempts from disclosure "[r]ecords, the disclosure of which is exempted or prohibited pursuant to federal or state law, including, but not limited to, provisions of the Evidence Code relating to privilege." Trade secrets are privileged under Evidence Code §1060 and are therefore protected from disclosure pursuant to §6254(k). *See, e.g.*, *Uribe v. Howie*, 19 Cal. App. 3d 194, 206 (1971). Under these provisions, trade secrets are accorded near absolute protection, rather than being subject to a public interest balancing test, and may not be disclosed unless failure to do so would "conceal fraud" or otherwise result in a "serious injustice." *Bridgestone/Firestone, Inc. v. Superior Court*, 7 Cal.App.4th 1384, 1391, (1992), *reh'g denied and opinion modified* (July 23, 1992); Evid. Code §1060. Because a different set of legal principles governs the disclosure of competitively sensitive data that constitutes a trade secret, it is appropriate for the Commission to adopt a confidential matrix for such data, in addition to one for competitive data that may not meet the definition of a trade secret but is otherwise deserving of protection §6255(a).

The creation of such a matrix is important because a significant portion of the data that TNCs are compelled to produce to the Commission constitutes extremely valuable and sensitive trade secret information. In Decision (D.)13-09-045, the Commission ordered TNCs to provide periodic verified reports to the Commission's Safety and Enforcement Division (SED) that include specified categories of information concerning their operations.[2] In recognition of the sensitive nature of this information, the decision expressly required TNCs to file these reports confidentially. *Id.*[3] Much of this data constitutes a trade secret because it reveals critical metrics of the unique transportation network company business that could be used to determine a competitor's market share and to evaluate the effectiveness of its marketing and promotional efforts, thereby allowing the competitor to more effectively deploy its own resources to gain market share.

A trade secret is "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[4] A key example of TNC data that constitutes a trade secret is the electronic "trip data" collected by TNCs in the course of their operations, much of which is reported to the Commission in the form of a massive data file containing data regarding every pick-up and drop off completed by the TNC during the reporting period.[5] TNCs continually collect a series of data points regarding trips completed on the platform, including the time and location of the request, the location of the driver, the pick-up and drop-off location, the miles traveled and the fare because, among other reasons, the success of the business model depends upon continually optimizing the balance between passenger demand for rides and the supply of vehicles and drivers necessary to meet that demand. Members of the TNC Working Group endeavor to optimize supply and demand by continually tweaking their pricing and promotional activities, using ride credits and other discounts to stimulate passenger demand, while increasing

[2] D.13-09-045, p. 31.
[3] The Commission stated in D.13-09-045 that "[f]or the requested reporting requirements, TNCs shall file these reports confidentially unless in Phase II of this decision we require public reporting from TCP companies as well." The Commission did not impose any public reporting requirements in Phase II, or otherwise impose any such requirements.
[4] Civil Code § 3426.1.
[5] *See* D.13-09-045, at pp. 31-32.

the supply of vehicles to areas with high demand by offering driver incentives. Analysis of electronic trip data enables TNCs to dynamically adjust these two levers in real time to ensure that fares are ***low*** enough to attract passengers while fares are ***high*** enough to attract drivers. Striking this delicate balance is central to a TNC's ability to remain competitive.

The collected electronic trip data allows TNCs to continually evaluate the effectiveness of their promotional, advertising and incentive campaigns used to balance supply and demand. For example, by comparing the number of rides completed during a particular time period in a particular location against the driver incentive programs deployed during that period, a TNC 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 its ride numbers against the particular passenger promotions run at that time, TNCs can track, assess, and understand the efficacy of their passenger-directed promotions, and can adjust them accordingly. Just as importantly, the TNC can identify those promotions that are ***ineffective*** and can avoid further expenditures on those promotions, conserving precious financial resources.

Not coincidentally, this data is also among the most competitively sensitive forms of data maintained by a TNC because the TNC's competitors (not just other TNCs but also taxis, rail, TCPs, etc.) could use that very same data to reverse engineer the effectiveness of its pricing, promotional activity and product positioning. Competition is fierce among TNCs and the potential gains from access to competitively sensitive information are immense. If a competitor were provided with access to its ride data, it could and would compare that data to the TNC's driver acquisition programs and passenger promotions – which, by their nature, are publicly discoverable – to better understand which of these strategies are effective. This would allow the competitor to tailor its operations to compete more effectively, utilizing for its own benefit data that the TNC has generated over time and at great expense. Such a competitor could avoid investing the significant resources invested by the TNC in testing these programs and analyzing the data itself. At the same time, a new competitor could enter the market without substantial investment, "free-riding" on the efforts of companies who have done the hard work to win over customers and build their brands.

In addition to electronic trip data, TNCs maintain other forms of competitively sensitive information that may be reported to the Commission, including, without limitation, data regarding the number of drivers completing driver training programs, data regarding the number of miles and hours driven by drivers, and data regarding the TNC's handling of incidents on the platform. This data is also a trade secret because it serves as a proxy for the TNC's market share, customer growth, and revenue figures, or because it may disclose the TNC's proprietary processes for addressing user complaints or incidents on the platform. Other forms of data maintained by TNCs that is subject to trade secret protection include undisclosed new business initiatives, financial projections, proprietary insurance products, and nonpublic financial data. Because of the extreme sensitivity of this data, TNCs jealously guard its secrecy, limiting access internally on a need to know basis and applying other security measures to keep it from being publicly disclosed, including nondisclosure agreements and technical, physical and administrative safeguards.

Because the data described above derives tremendous value from not being known by competitors and is the subject of rigorous efforts to maintain its confidentiality, the data qualifies for protection as a trade secret under Civil Code § 3426.1 and relevant decisional law. *See, e.g.*, *Lion Raisins Inc. v. USDA*, 354 F3d 1072, 1080-81 (9th Cir 2004) (where information collected by agency would allow competitor to "infer critical information about its competitors' volume, market share, and marketing strategy," agency appropriately refused to produce in response to Freedom of Information Act request); *Mattel, Inc. v. MGA Entm't, Inc*., 782 F.Supp.2d 911, 972 (C.D.Cal.2011) ("This information has potential or actual value from not being generally known to the public: information about customers' preferences can aid in 'securing and retaining their business.'"); *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 521 (9th Cir. 1993) ("The Customer Database has potential economic value because it allows a competitor like Peak to direct its sales efforts to those potential customers that are already using the MAI computer system."); *National Information Center, Inc. v. American Lifestyle*, 227 U.S.P.Q. 460, 1985 WL 4035 (E.D. La. 1985) (trade secret protection extended to advertising, market studies used in developing advertisements, and to data, internal codes and methods of allocation used in accounting and control procedures); *Editions Play Bac, S.A. v. Western Pub. Co., Inc.*, 31 U.S.P.Q.2d 1338, 1342 n.3 (S.D. N.Y. 1993) ("'how and why' behind marketing strategies" protectable as trade secret); *Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1443, 1155 (4th Dist. 2002) ("pricing concessions, promotional discounts, advertising allowances, volume rebates, marketing concessions, payment

terms and rebate incentives …[have] independent economic value because Schlage's pricing policies would be valuable to a competitor to set prices which meet or undercut Schlage's."); *Brunswick Corp. v. Jones*, 784 F.2d 271, 275 (7th Cir. 1986) (confidential information concerning plaintiff's financial performance and projections and marketing plans would help competitor to determine how aggressively it should price new products and to preempt plaintiff's new products before they reached the market); *Black, Sivalls & Bryson, Inc. v. Keystone Steel Fabrication, Inc.*, 584 F.2d 946, 952 (10th Cir. 1978) (confidential data regarding operating and pricing policies can qualify as trade secrets, because the ability to predict a competitor's bid with reasonable accuracy would give a distinct advantage to the possessor of that information).

Because the above-described data constitutes trade secret information, it is exempt from disclosure under the Public Records Act and may not be disclosed unless to do otherwise would conceal a fraud or work a serious injustice. Gov. Code §6254(k); Evid. Code §1060; *Bridgestone/Firestone,* 7 Cal.App.4th at 1391. It is therefore appropriate for the Commission to adopt a confidential matrix that reflects the more rigorous standard applicable to competitively sensitive materials that qualify as trade secrets under Evidence Code §1060,[6] in addition to a matrix covering competitive data that may not qualify as a trade secret but is entitled to protection under §6255(a).

2. Customer/user activity files protected under Gov't Code §6254(c) and Gov't Code §6254(k)

The ACR proposes a matrix covering "personally identifiable information of regulated entity customers protected by Gov't Code § 6254(c)." The TNC Working Group strongly supports creating a matrix to protect the private information of users, however, the TNC Working Group is concerned that the articulation of the category in the ACR may be too narrow to embrace the types of private, personal data regularly collected and maintained by TNCs. The TNC Working Group therefore proposes that the Commission either confirm that the proposed category covers the kinds of personal data maintained by TNCs or, in the alternative, that the Commission adopt a separate category to cover such data.

[6] The TNC Working Group will identify subsets of data falling within this matrix category more particularly in its October 3 submission, but suggests here the following possible subcategories: (a) Trip data and other data collected through the TNC's proprietary technology; (b) Data that would reveal market share or promotional efforts; (c) Proprietary internal processes; (d) Customer lists; (e) Undisclosed business opportunities or financial projections; (f) Nonpublic financial information; and (g) Proprietary, nonpublic insurance products.

TNCs routinely collect and maintain various forms of private personal data regarding individuals who use the TNC platform to give or receive rides. In addition to collecting the usual contact information received by many regulated entities – e.g., name, address, telephone number, payment information -- TNCs also collect social security numbers and driver's license numbers of drivers in order to retrieve highly sensitive records of user driving history and criminal history. TNCs need to have this information to comply with regulatory requirements to check a driver's driving record and perform mandated background checks. In addition, in the course of their operations, TNCs continually collect electronic records of driver activity on the platform, including a record of trips completed, promotions, earnings and payments received, complaint history, communications and internal notes regarding the driver, and a record of any adverse actions taken by the TNC against the driver (e.g., removing a driver's access to the TNC app). With respect to riders, TNCs maintain records of all rides received -- including precise GPS data of pick-ups, drop-offs and routes taken -- as well as a record of communications with the rider and any incident reports submitted by or concerning him or her. The records maintained by TNCs regarding both drivers and passengers are akin to "customer files" maintained by other regulated entities and fall squarely within the protections offered by §6254(c), which exempts from disclosure "[p]ersonnel, medical, ***or similar files***, the disclosure of which would constitute an unwarranted invasion of personal privacy."[7] Because the disclosure of such data would constitute an unwarranted invasion of personal privacy, it is likewise subject to protection under Gov't Code §6254(k) and the personal right of privacy guaranteed by the California Constitution. Cal. Const. Art. I, § 1; *Versaci v. Superior Court,* 127 Cal.App.4th 805, 812–13 (2005) (California Constitution contains an explicit right of privacy that operates to protect the private, personal information of individuals). *Hill v. National Collegiate Athletic Assn.*, 7 Cal. 4th 1, 35 (1994) (The right of privacy protects against the unwarranted dissemination or misuse of sensitive and confidential information, while preserving the right of individuals to conduct "personal activities without observation, intrusion or interference."); *City of Carmel–by–the–Sea v. Young*, 2 Cal. 3d 259, 268 (1970) ("[T]he protection of one's personal financial affairs ... against compulsory public disclosure is an aspect of the zone of privacy…"); *Board of Trustees v. Superior Court*, 119 Cal.App.3d 516, 525–26 (1981) ("The custodian [of private information] has the right, in fact the duty, to resist attempts at unauthorized disclosure and the person who is the subject of [it] is

[7] Emphasis added.

entitled to expect that his right will be thus asserted."). As a result, the TNC Working Group ***presumes*** these files would be covered by the matrix proposed in the ACR, which clearly appears to be designed to protect the private, personal information of the customers/users of regulated entities from being publicly disclosed.

The TNC Working Group is uncertain, however, whether the ACR's reference to the term "personally identifiable information" might be construed as a limitation on the kinds of data covered by the matrix in a way that excludes the user activity files maintained by TNCs. This is because there is no universally accepted definition of the term PII. PII has been defined in various ways depending upon the context in which it is used. For example, the definitions included in the California Online Privacy Protection Act and the California data breach notification law are focused on personal contact information, financial account or social security numbers, and online identifiers (*see, e.g.*, Bus. & Prof. Code, § 22577 and Bus. & Prof. Code, § 22947.1), while the definition of PII in §31490 of the Streets and Highways Code, a provision aimed at limiting disclosure of data collected by bridge and highway toll collectors, includes "any information that identifies or describes a person including, but not limited to, travel pattern data, address, telephone number, email address, license plate number, photograph, bank account information, or credit card number." Sts. & Hy. Code, § 31490. Meanwhile, the definition of PII in the federal Video Privacy Protection Act is narrowly focused on "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C.A. § 2710. And the definition of PII in the Family Educational Rights and Privacy Act ("FERPA") is focused primarily upon student, parent or family member names or addresses, biometric records, and indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name. 34 C.F.R. § 99.3. In contradistinction to these more contextual definitions, the Federal Trade Commission, on the other hand, has advocated for a more expansive, definition of PII as including any information reasonably capable of being identified to an individual person or device.[8]

[8] *See* Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, May 27, 2016 at https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf, p. 10.

Given these varying definitions of PII, the TNC Working Group is uncertain as to the scope of the §6254(c) matrix proposed in the ACR or whether it is intended to include the kinds of private personal customer data otherwise subject to protection under 6254(c). For that reason, the TNC Working Group requests that the Commission either clarify that the matrix for "personally identifiable information of regulated entity customers protected by Gov't Code § 6254(c)" covers the activity of customers/users of regulated entities, including TNC data regarding users' activity on the platform (either explicitly or by adopting the definition of PII proposed by the FTC); or alternatively, that the Commission adopt a separate matrix for TNC customer/user activity files protected by §6254(c), which would cover that data.

3. Records of user incident reports protected under GC §6254(c) and/or GC §6255(a)

The TNC Working Group proposes that the Commission adopt a confidential matrix for TNC user incident reports subject to nondisclosure under GC §6254(c) and/or §6255(a).[9] In the course of their operations and pursuant to Commission regulations, TNCs regularly receive, investigate and resolve user incident reports, and much of this data is required to be reported to the Commission; some of it in the form of periodic reports and some in response to targeted data requests issued by staff. These customer incident reports include reports of suspected drug or alcohol use by drivers or passengers (including "zero tolerance" reports required under D.13-09-045), vehicle accident reports, and other kinds of incident reports and customer complaints. TNCs receive these reports through various means, including in-app messaging, user reviews, and critical response lines maintained specifically for this purpose. Providing multiple, user-friendly avenues for users to report concerns regarding activity on the platform encourages the free flow of information and allows TNCs to promptly investigate these reports and take action to address them, or to otherwise provide assistance to users of the platform. Thus, these incident reporting mechanisms play an important role in allowing TNCs to monitor and regulate activity on the platform and to ensure the safety and security of their users.

The information gathered in connection with these incident reports includes highly sensitive personal information regarding TNC users. These files often include uncorroborated

[9] Although these files could potentially be included within the category discussed in section 2 above regarding "customer files," the data discussed herein is often maintained and reported outside of any particular user's file; for example, in zero tolerance reports, which take the form of an electronic file with data regarding all such reports received during the reporting period for all users of the platform.

allegations concerning alleged misconduct by users of the platform, as well as notes regarding the TNC's investigation of the incident and any remedial action taken to resolve the issue. As a result, incident files may include embarrassing or potentially libelous allegations against users -- a significant portion of which prove to be wholly unsubstantiated. The public disclosure of these raw, uncorroborated and potentially libelous allegations would plainly constitute an unwarranted invasion of user privacy. As a result, user incident files are protected from disclosure pursuant to 6254(c), as well as the public interest balancing test of §6255(a).

Section 6255(c) exempts from disclosure "[p]ersonnel, medical, or ***similar files***, the disclosure of which would constitute an unwarranted invasion of personal privacy."[10] TNC user incident files are "similar" to personnel files in relevant respects and the public disclosure of these files could subject users to embarrassment or public ridicule, or may otherwise result in an unwarranted invasion of user privacy; for example, by disclosing sensitive geolocation information associated with an incident. They should therefore be protected from disclosure under §6254(c).

TNC user incident files should also protected from disclosure under §6255(a), the public interest balancing test, as there is a strong public interest in maintaining the confidentiality of unverified allegations of unlawful or inappropriate activity. *See, e.g., Chronicle Pub. Co. v. Superior Court In and For City and County of San Francisco,* 54 Cal. 2d 548, 569 (1960) (holding that public interest in secrecy of state bar complaints outweighed need for access, noting "[t]he fact that a charge has been made against an attorney, no matter how guiltless the attorney might be, if generally known, would do the attorney irreparable harm even though he be cleared by the State Bar."); *American Civil Liberties Union Foundation v. Deukmejian,* 32 Cal. 3d 440, 451 (1982) (raw "intelligence information" regarding suspected organized crime figures not subject to disclosure under PRA on the grounds, *inter alia*, that "persons seeking to damage the reputation of another may try to discover if he is listed as an organized crime figure or as an associate of such a figure….").

There is an equally strong public interest in maintaining the free flow of user complaints to TNCs so that they can quickly take action to investigate and address them; including, where appropriate, taking immediate action to revoke a user's access to the platform for the safety of other users and the general public. *Terzian v. Superior Court*, 10 Cal. App. 3d 286, 295–96 (1970)

[10] Govt Code §6254(c) (emphasis added).

("It is also generally recognized that when the public interest in securing information necessitates the free communication of such information on a privileged, confidential basis, disclosure of information so secured is against the public interest."). The public disclosure of user incident files could discourage users from notifying TNCs of suspected inappropriate activity by, for example, exposing a complaining user to undesired public scrutiny, a potential defamation claim, or another form of retaliation. *See*, e.g., *City of San Jose v. Sup. Ct.*, 74 Cal. App. 4th 1008, 1023 (1999) (producing complaints submitted by members of the public may "have a chilling effect on complaints, because the newspaper's purpose in obtaining their identify is to contact complainants directly" and "citizens who wish to make an airport noise complaint will have no choice but to remain silent while maintaining their privacy, or else register their complaints at the risk of being questioned in their homes by the press or other persons as to whether they are telling the truth"); *Chronicle Pub. Co.*, 54 Cal. 2d at 568 ("'If every citizen who knows of the unfitness of an officer or employe (sic), or of facts he thinks require an investigation, believes it his duty to lodge information before the board, he will hesitate a long while before doing so if he knows his complaint is to be made public and become of the public records, so that any one may have access to it and he subjected to action for a possible libel. It is not to be expected, if that is so, that very many will come forward and lodge a complaint."); *cf Black Panther Party v. Kehoe*, 42 Cal. App. 3d 645, 658 (1974) (practice of disclosing complaints "serves to discourage complaints because it defeats the provisional assurances of confidentiality which section 6254, subdivision (f), offers to complaining citizens."); *Haynie v. Superior Court*, 26 Cal. 4th 1061, 1070–71 (2001) ("Complainants and other witnesses whose identities were disclosed might disappear or refuse to cooperate…. Citizens would be reluctant to report suspicious activity.").

As the foregoing cases illustrate, the public disclosure of user incident reports would harm TNC users by subjecting them to unwarranted embarrassment or ridicule from the publication of unsubstantiated allegations of wrongdoing. Disclosure of these reports is also likely to discourage TNC users from freely reporting incidents on the platform for fear of retaliation or unwanted public scrutiny; inhibiting the ability of TNCs to police their platforms and ensure the safety of their users (both riders and drivers). Thus, there is a strong public interest in maintaining the confidentiality of these files. In contrast to the strong public interest in nondisclosure, there is little, if any, public interest in disclosing the substance of such files beyond a prurient interest in

sensational but unproven allegations against TNC users, or other nefarious purposes. For all of these reasons, the user incident files are subject to protection from disclosure pursuant to §6255(a).

The TNC Working Group therefore urges the Commission to adopt a confidential matrix for TNC user incident files subject to protection under Gov't Code §6254(c) and Gov't Code §6255(a).

4. CPUC annual reports submitted under assurances of confidentiality and related supplemental data requests

The TNC Working Group also proposes that the Commission adopt a confidential matrix for CPUC annual reports and related supplemental data requests that have been submitted confidentially pursuant to and in reliance upon CPUC regulations. In D.13-09-045, the Commission ordered TNCs to submit annual verified reports to the SED that include specified categories of information concerning their operations.[11] The Commission expressly ordered TNCs to file these reports confidentially given the highly sensitive nature of the data included in the reports, including many of the data elements discussed above.[12] In accordance with and in reliance upon D.13-09-045, the TNC Working Group members have dutifully submitted such reports confidentially and with the expectation that they would not be publicly disclosed. Members of the TNC Working Group have also been required to respond to supplemental, follow-up data requests regarding the aforementioned annual reports, to which they have also responded confidentially in reliance upon D.13-09-045. Because the data in these reports arises from and relates to the data in the annual reports and was submitted under compulsion of law and in reliance upon Commission assurances of confidentiality, it would be inappropriate for the Commission to disclose the data in response to public requests for access to the data. *See, e.g.*, *See, e.g.*, *Johnson v. Winter*, 127 Cal.App.3d 435, 439 (1982) (strong public interest in nondisclosure of information submitted under assurances of confidentiality); *Syngenta Crop Protection, Inc. v. Helliker,* 138 Cal.App.4th 1135, 1167-68 (2006) (*citing Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1003–1005-1011 (1984)) (where company had "reasonable investment-backed expectation of confidentiality" in data submitted to agency, use of that data to benefit competitor constitutes unlawful taking). The Commission should therefore adopt a confidential matrix for data submitted by TNCs pursuant to

[11] *See* D.13-09-045, p. 31.

[12] The Commission stated in D.13-09-045 that "[f]or the requested reporting requirements, TNCs shall file these reports confidentially unless in Phase II of this decision we require public reporting from TCP companies as well." The Commission did not impose any additional public reporting requirements in Phase II, and has not otherwise imposed any such requirements.

D.13-09-045, specifically including data contained in required annual reports and related supplemental data requests, specifying that such data is confidential and will not be disclosed.

Dated: September 22, 2017 **BRYAN CAVE LLP**

By: */S/*
Daniel Rockey
Attorneys for Lyft, Inc.