QUINN EMANUEL URQUHART & SULLIVAN, LLP
James R. Asperger (Bar No. 83188)
jimasperger@quinnemanuel.com
Stephen A. Broome (Bar No. 314605)
stephenbroome@quinnemanuel.com
Lauren B. Lindsay (Bar No. 280516)
laurenlindsay@quinnemanuel.com
William R. Sears (Bar. No. 330888)
willsears@quinnemanuel.com
865 South Figueroa Street, 10th Floor
Los Angeles, California 90017-2543
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Attorneys for Defendants TWC PRODUCT AND TECHNOLOGY, LLC and INTERNATIONAL BUSINESS MACHINES CORPORATION

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES

THE PEOPLE OF THE STATE OF CALIFORNIA,

Plaintiff,

vs.

TWC PRODUCT AND TECHNOLOGY, LLC, a Delaware corporation; INTERNATIONAL BUSINESS MACHINES CORPORATION, a New York corporation; and DOES 2-50, inclusive,

Defendants.

CASE NO. 19STCV00605

DEFENDANTS' NOTICE OF MOTION AND MOTION FOR SUMMARY JUDGMENT ON PLAINTIFF'S UCL CAUSE OF ACTION

[*Separate Statement of Undisputed Facts, Declaration of Krista Rouse, Declaration of Lucas Cyr, Declaration of Lauren Lindsay, Declaration of Karl Snow, Request for Judicial Notice, and Appendix of Exhibits filed concurrently*]

Assigned for All Purposes to the Hon. Mark V. Mooney
Dept. 68

Date: TBD
Time: TBD

Action Filed: January 3, 2019
Trial Date: January 25, 2021

NOTICE OF MOTION AND MOTION

TO THIS HONORABLE COURT, ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on _____, _____, 2020, at ___ a.m.,[1] or as soon thereafter as the matter may be heard in Department 68 of the above-entitled Court, located at 111 North Hill Street, Los Angeles, California 90012, Defendants TWC Product & Technology, LLC ("TWC") and International Business Machines Corporation ("IBM") will, and hereby do, move the Court pursuant to California Code of Civil Procedure section 437c, for summary judgment as to the Complaint filed by plaintiff The Los Angeles City Attorney on behalf of the People of the State of California ("Plaintiff"). Defendants are entitled to summary judgment on Plaintiff's sole claim for violations of Business and Professions Code section 17200 on the following grounds based on the undisputed facts and as a matter of law: (1) Plaintiff cannot establish that Defendants engaged in fraudulent conduct; and (2) Plaintiff cannot establish that Defendants engaged in unfair conduct.

This Motion is based on this Notice; the accompanying Memorandum of Points and Authorities in support thereof; the concurrently filed Separate Statement of Undisputed Facts, the Declarations of Krista Rouse, Lucas Cyr, Lauren Lindsay, and Karl Snow; the Request for Judicial Notice; the Appendix of Exhibits; the pleadings and other papers on file in this action; and such other declarations, evidence and argument as may be presented at or before the hearing.

[1] As of the date of this Motion's submission, the Los Angeles Superior Court's hearing reservation system remains unavailable due to the COVID-19 pandemic. *See* Court Reservation System, *available at* https://portal-lasc.journaltech.com/public-portal/?q=node/388 ("The Court Reservation System is unavailable until further notice. During the COVID-19 pandemic and the period of time during which the court's operations are limited pursuant to the Presiding Judge's General Orders, parties will be unable to reserve hearing dates online. . . . In the meantime, litigants may continue to electronically file documents without a CRS hearing date until further notice."). Once the system permits Defendants to reserve a hearing date for the Motion, they will serve notice of the hearing date and time.

DATED: June 11, 2020

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By /s/ *Stephen A. Broome*
James R. Asperger
Stephen A. Broome
Lauren B. Lindsay
William R. Sears

Attorneys for Defendants
TWC PRODUCT AND TECHNOLOGY, LLC
INTERNATIONAL BUSINESS MACHINES CORPORATION

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutory Authorities

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

PRELIMINARY STATEMENT

Discovery has definitively proven that this lawsuit was filed on a false premise. When the Los Angeles City Attorney filed his Complaint almost a year and a half ago—based largely on a New York Times exposé, *see* Ex. 1 (Compl.) ¶ 5—his central premise was that Defendants deceived users of "The Weather Channel App" (the "TWC App" or the "App") into sharing their location data with the App. Specifically, he asserted that users would not have agreed to share their location data if Defendants' use and sharing of that data for advertising purposes had been disclosed *in the App's location-access permission prompt* (as opposed to in the App's Privacy Policy, where the information indisputably *was* disclosed in conformance with applicable California law). *Id.* ¶¶ 45-46. But the actual behavior of TWC App users proves otherwise. In the Spring of 2019 (a few months after Plaintiff filed suit), Defendants showed a new disclosure screen to all new and existing users that (1) specifically disclosed the allegedly omitted information, and (2) required users to click "I understand" before proceeding to the location-access permission prompt. Analysis of user-session data that reflects TWC App users' location permission settings over time (the "Sessions Data") shows that, after Defendants specifically alerted users to the allegedly omitted information, they continued sharing their device's location data with the App at essentially the *same* rate. In other words, the allegedly omitted information had no material impact on users' decisions. The Sessions Data guts the underlying premise of Plaintiff's lawsuit and forecloses his claims under the "fraud" and "unfair" prongs of the Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq*.) ("UCL").

The results of the Sessions Data are not surprising given the undisputed fact that, during the relevant period, Defendants *did* disclose the information that Plaintiff alleges was omitted from the App's location-access permission prompt—in the App's online Privacy Policy, links to which were provided on the App's download page and in multiple locations within the App. Thus, users concerned about how their data might be used had easy access to the allegedly omitted information. There is no dispute that Defendants' Privacy Policy fully complied with California's operative data privacy disclosure law during the relevant period—*i.e.*, the California Online Privacy Protection Act

(Cal. Bus. & Prof. Code §§ 22575, *et seq.*) ("CalOPPA")—which requires businesses to disclose the information at issue in an online privacy policy, as Defendants did. According to the Legislature, CalOPPA "provides *meaningful privacy protections* . . . by allowing individuals to rely on a privacy policy posted online." Ex. 4 (Assem. Com. on Judiciary, Analysis of Assem. Bill No. 68 (2003-2004 Reg. Sess.) as amended Apr. 2, 2003) at AE 75 (emphasis added).

Plaintiff disagrees with the Legislature, and contends that information disclosed in a privacy policy—even a CalOPPA-compliant one like Defendants'—is "*not* meaningfully conveyed" because "reasonable users" are "not likely to read" privacy policies.[2] Plaintiff asks the Court to disregard CalOPPA in favor of applying substantially more rigorous and detailed disclosure requirements that, Plaintiff contends, are implied in the UCL—a statute that the California Supreme Court recently observed uses "exceedingly broad and general language." *See Nationwide Biweekly Admin., Inc. v. Sup. Ct. of Alameda Cty.*, 9 Cal. 5th 279, 300 (2020). Plaintiff asserts that, to comply with these purported UCL-implied disclosure requirements, Defendants had to disclose their use and sharing of location data for advertising not merely in their Privacy Policy but *also* in the permission prompt (or another "conspicuous location that reasonable users are likely to read," Ex. 1 (Compl.) ¶¶ 45-46), and that Defendants violated the UCL by failing to do so.

That Plaintiff's claim amounts to second-guessing the California Legislature's judgment regarding the appropriate form, content, and location of data privacy disclosures—as reflected in CalOPPA, and more recently, in the California Consumer Privacy Act (Cal. Civ. Code §§ 1798, *et seq.*) ("CCPA")—is the subject of Defendants' concurrently-filed Motion for Summary Judgment on Defendants' Affirmative Defense of Equitable Abstention ("Abstention MSJ"). The Abstention MSJ asks the Court to abstain from implying in the UCL detailed data privacy disclosure requirements that substantially exceed and conflict with those set forth in CalOPPA and the CCPA, as ruling in Plaintiff's favor would require the Court to do. Even if the Court were not to abstain,

[2] *See* Ex. 2 (Plaintiff's Responses And Objections To Defendant IBM's First Set of Special Interrogatories ("Plaintiff's Rog Responses"), at Response No. 3) at AE 40-45; *see also* Ex. 1 (Compl.) ¶ 7.

however, summary judgment should still be granted and the case dismissed because the undisputed facts establish that Plaintiff cannot prove the elements of his claim under either asserted prong.

***Fraud Prong*:** Plaintiff does not allege that Defendants made any affirmative misrepresentations, and instead asserts a "failure-to-disclose" theory. According to Plaintiff, Defendants failed to disclose their use and sharing of location data for advertising purposes *in the App's location-access permission prompt*. Ex. 1 (Compl.) ¶ 7. But there was no "failure to disclose" here because it is undisputed that Defendants disclosed this information in their Privacy Policy—the very location that the Legislature determined such information *should* be disclosed and where reasonable users should expect to find it.

Moreover, any alleged "omission" in the permission prompt was immaterial, as proven by an analysis conducted by Defendants' expert, Dr. Karl Snow, of the Sessions Data described above (and in more detail below). In order for Plaintiff to prove that the information allegedly omitted from the permission prompt was material to users' decisions to share their location data, Plaintiff would have to show that Defendants' specific disclosure of that *exact* information in the new disclosure screens caused a substantial *decrease* in the rate at which users shared their location. As Dr. Snow explains, the Sessions Data shows that there was no material change in that rate.

***Unfair Prong*:** Plaintiff's unfair prong claim is also meritless. To begin with, Plaintiff cannot establish the requisite "substantial injury" to consumers. Indeed, Plaintiff *admits* that some users would consider the alleged harm—*i.e.*, Defendants' use of location data to provide potentially more relevant ads—to be a "benefit." Against this admitted benefit, Plaintiff identifies only subjective and speculative emotional harms that do not amount to a "substantial injury" as a matter of law. Nor can Plaintiff establish the element of causation, given that the Sessions Data shows that users made the same choice once the allegedly omitted information was specifically brought to their attention. Finally, users could reasonably have avoided any purported "injury" simply by reviewing TWC's Privacy Policy. The unfair prong claim may be dismissed on any one of these bases.

Accordingly, the Motion should be granted and Plaintiff's claim dismissed.

FACTUAL AND LEGAL BACKGROUND

A. The TWC App Uses Location Data To Provide Users With Localized Weather Information And Tailored Advertisements

The TWC App is available for download on Android (Google) and iOS (Apple) devices and provides users with state-of-the-art weather forecasts, alerts, and other real-time weather information based on device location. UF ¶¶ 1-3. The Android and iOS operating systems can determine the precise geographic latitude and longitude of a mobile device through the use of location-based services such as Global Positioning System ("GPS") sensors. UF ¶ 7. The operating systems display a "permission prompt" to which the user must consent before the operating systems will allow an app to access the latitude and longitude data of a mobile device. UF ¶¶ 8-9. If the user declines consent, the app cannot access this data. UF ¶¶ 9-10. If the user consents to allowing the TWC App to access their device's location, the App accesses the data and provides automatically localized weather data, alerts and forecasts. UF ¶ 10. Users are not required to share their location in order to use the App; if they decline, they can manually enter a location to see the weather forecast for that area. UF ¶ 11.

At the time Plaintiff filed suit, the TWC App did not (and still does not) allow users to create profiles that include names or other identifying information such as addresses, phone numbers, or email addresses.[3] UF ¶ 27. Each installation of the App is associated with an Advertising ID randomly assigned to a device by the device's operating system (*e.g.*, Android or iOS). UF ¶ 29.

The App costs Defendants tens of millions of dollars per year to operate, but is provided to users free of charge. UF ¶ 4. Unless a user has paid a fee to remove ads, each time a user opens the App, an ad appears just below the weather forecast. UF ¶¶ 6, 16. The ad revenue pays the costs of operating the App. UF ¶ 5.

Users receive ads through the App whether or not they choose to allow the App to access their device's GPS. UF ¶ 17. If a user allows such access, Defendants may use that location data

[3] Until May 2018, TWC App users had the *option* to create a profile and enter certain contact information. UF ¶ 28. Very few users actually created profiles. In March 2018, only 4.5% of the monthly active users ("MAU") on TWC's iOS App and 3.9% of the MAU on TWC's Android App had profiles. *Id.* Plaintiff does not make any allegations regarding this information.

to tailor the ads that the App displays. UF ¶ 14. For example, advertisers may contract with TWC to deliver their ads only to TWC App users at or near certain locations where the advertisers' products or services are available. UF ¶ 15. Or, advertisers may contract with TWC to deliver ads only to users who recently visited, or routinely visit, certain commercial points of interest (*e.g.*, a golf course or a coffee shop) to increase the chance of reaching consumers that are interested in the advertisers' products or services (*e.g.*, golf lessons, or a discount code for Starbucks coffee). UF ¶ 15.[4] Thus, if a user allows the App to access their device's GPS, the App uses that information to provide ads that are potentially more relevant to the user. Plaintiff admits that some users would consider such location-tailored advertising to be a "benefit." UF ¶ 18.

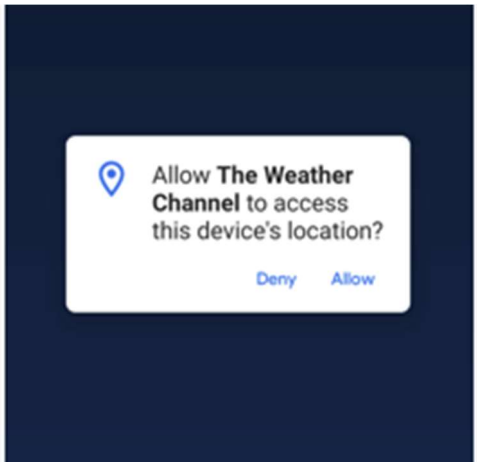
Defendants share location data with certain partners that provide services related to the App (which is not a sale of location data). UF ¶¶ 19-20. There is no evidence that any location data collected through the App has ever been used to identify an individual user, or compromised by a data breach or hack, either through Defendants' systems or those of any of Defendants' partners. UF ¶ 33.

B. The App's Location-Access Permission Prompts, Privacy Policy, And In-App Disclosures

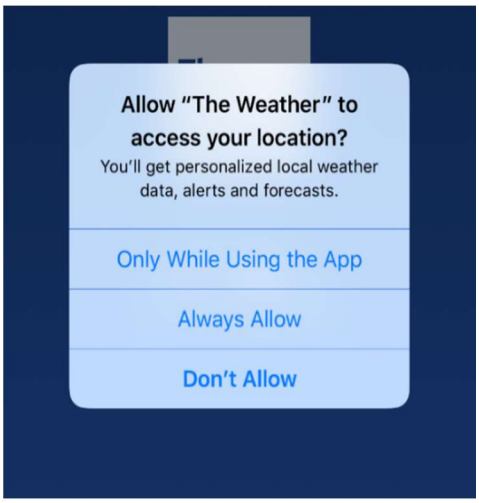
At the time Plaintiff filed suit, the first time a user opened the App, a prompt was displayed that requested permission to access their device's location. UF ¶ 9. This prompt was generated by the device's operating system (Android or iOS) and required affirmative consent to access the location data (latitude and longitude coordinates) generated by the device's GPS. The prompts in effect at the time Plaintiff filed the Complaint are shown below. UF ¶¶ 34, 37; *see also* Exs. 11, 12. Google supplied the text of the Android prompt (with the exception of the app's name) and did not permit app developers to modify it. UF ¶ 35. Apple also supplied the initial text of the iOS prompt, but permitted developers to add some text. UF ¶ 36.

[4] The commercial points of interest purposely do not include sensitive locations that would give rise to privacy concerns, such as churches, schools, or health care facilities. UF ¶ 32.

Android Permission Prompt



iOS Permission Prompt



Plaintiff alleges that Defendants violated the "fraud" and "unfair" prongs of the UCL by failing to disclose in the foregoing permission prompts (or a similar "pop-up" screen) the fact that location data shared with the App may be used for advertising and shared with certain of Defendants' partners that provide services for the App. Ex. 1 (Compl.) ¶¶ 45-46.

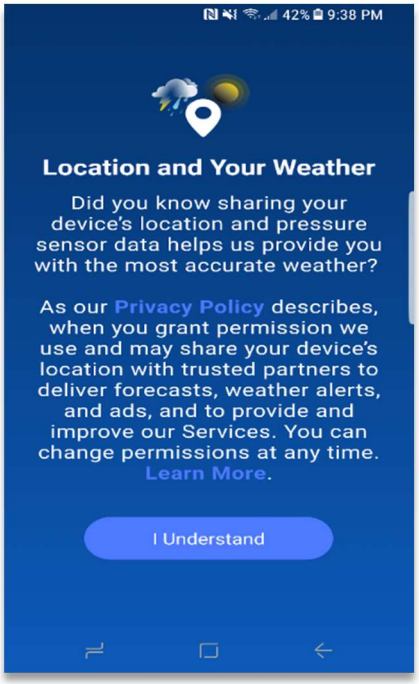
Defendants, however, actually *did* disclose this exact information where consumers concerned about the privacy of their data would expect to find it—in the App's Privacy Policy. UF ¶ 21. The Privacy Policy in effect at the time Plaintiff filed suit stated that: "We, our service providers, and our Ad and Analytics Partners . . . may collect location information through the Services. ***We may share the location information we collect with third parties*** . . . . We collect location information to provide you with location-based services (such as severe weather alerts and other weather information through our mobile applications), ***provide advertisements that are relevant to your geographic location***, and conduct analytics to improve the Services." Ex. 13 at AE 574 (emphasis added). The Privacy Policy further explained that "we may also provide to Ad Partners . . . information [that] may include data about . . . physical places users have visited." *Id.* at AE 584. The other Privacy Policies in effect during the relevant period likewise disclosed the use and sharing of location data for advertising. Ex. 21; UF ¶ 21. The Privacy Policy was available for review through: (1) a link posted on the App's download pages, (2) various links within the App, including within the Settings menu, and (3) on the App's website. UF ¶¶ 22-23.

In addition, beginning in May 2018—*i.e.*, approximately seven months before Plaintiff filed suit—Defendants introduced a "Privacy Settings" screen, which also described the App's use and sharing of location data for advertising: "Allowing access to your device's location provides you with the most accurate weather forecasts, severe alerts, ***geographically relevant ads***, and content. ***We may also share location data with partners***, as described in our privacy policy." Ex. 14 (emphasis added); UF ¶ 24. The Privacy Settings screen included a "Learn More" link, which, when clicked, displayed a page that provided additional information regarding the App's use of location data for advertising purposes. Ex. 15; UF ¶ 25.

On January 24, 2019—three weeks after Plaintiff filed suit—Defendants revised the iOS App's location-access permission prompt to specifically mention the use and sharing of location data for advertising (consistent with plans devised before Plaintiff filed suit). *See* Ex. 16; UF ¶ 38. Defendants were unable to modify the Android App's location-access permission prompt because, as mentioned above, Google supplies the text of that prompt and does not permit app developers to modify it. UF ¶ 35.

On April 24, 2019, Defendants released a new version of the App for both iOS and Android that added a "Blue Screen" to the onboarding process. *See* Ex. 17; UF ¶ 39. As shown below, the Blue Screen: (1) specifically disclosed the App's use and sharing of location data for advertising; (2) provided a link to the App's Privacy Policy; (3) provided a "Learn More" link to a page that further describes the App's use and sharing of location data for advertising; and (4) required users to click "I Understand" before they could proceed to the location-access permission prompt. Exs. 17, 19; UF ¶¶ 39-41. Defendants showed the Blue Screen to all users who downloaded the App on or after April 24, 2019, *and to all pre-existing users* when they updated to the latest version of the App (which typically happens automatically).[5] UF ¶ 42.

[5] Approximately 75% of existing iOS App users updated the App within 17 days after the release of the April 24, 2019 version (version 10.9) of the iOS App and thus were presented with the Blue Screen and the second revised permission prompt. Approximately 75% of existing Android users updated the App within 28 days after the release of the April 24, 2019 version (version 9.5.0) and thus were presented with the Blue Screen. Ex. 23 (Snow Rept.) ¶¶ 44, 52 fn. 37; UF ¶¶ 43-44.



C. Dr. Snow's Analysis of TWC App Users' Sessions Data

Defendants' vendor, Localytics, maintains records of the location permission settings of the TWC App's daily active users—*i.e.*, the Sessions Data. UF ¶ 45. This data is generated for each user session, meaning it provides daily information regarding whether active users are sharing access to their devices' location-based services (*e.g.*, their device's GPS data). UF ¶ 46. Through the Sessions Data, it is possible to determine the percentage of active users consenting to share or declining to share such location data on a day-to-day basis. UF ¶ 48.

The Sessions Data can be used to test whether events such as Defendants' introduction of new disclosures in January and April 2019 had an effect on the rate at which users opted to share their location data with the App. Defendants retained Dr. Snow, a leading expert in the field of statistics, to conduct this analysis. Dr. Snow used widely accepted statistical methodologies, including event studies, to analyze the Sessions Data. *See* Ex. 23 (Snow Rept.) ¶¶ 23, 35-53.

Dr. Snow's analysis shows, *inter alia*, that, following Defendants' (1) January 24, 2019 revision to the iOS permission prompt to specifically mention the use and sharing of location data for advertising, and (2) April 24, 2019 launch of the Blue Screen that similarly disclosed such information to both iOS and Android users and required users to click "I Understand," there was no material change in the rate at which users shared their location data with the App. UF ¶ 47; Ex. 23

(Snow Rept.) ¶¶ 23, 35-53. Data on other metrics, such as App usage levels, downloads of the App, and uninstallations of the App similarly show no material change in response to these disclosures. UF ¶¶ 49-53; Ex. 23 (Snow Rept.) ¶¶ 23, 54-65, 66-77, 78-91.

D. The Statutory And Regulatory Regime Regarding Collection Of Personal Information

As discussed more fully in Defendants' concurrently-filed Abstention MSJ, the disclosures at issue here fall under a complex and evolving regulatory scheme. At the time Plaintiff filed this lawsuit, the location and content of online businesses' disclosures concerning the collection and use of consumer data was governed primarily by CalOPPA, which requires an operator of an online service that collects "personally identifiable information" to "conspicuously post its privacy policy on its Web site" or make the privacy policy available through "any other reasonably accessible means." Cal. Bus. & Prof. Code §§ 22575(a), 22577(b)(5). The privacy policy must disclose the "categories" of personal information that the business collects and the "categories" of third parties with whom the business may share that information. *See* Cal. Bus. & Prof. Code § 22575(b)(1). Plaintiff does not dispute that Defendants complied with CalOPPA at all relevant times. UF ¶ 54.

On June 28, 2018, the Legislature enacted the CCPA, which imposes more rigorous disclosure requirements, that are described in detail in the Abstention MSJ. In some circumstances, the CCPA implementing regulations will require a "just-in-time notice" (such as a pop-up screen), similar to the notice that Plaintiff claims Defendants should have provided in order to comply with the UCL. *See* Ex. 8, Regulation § 999.305(a)(4). However, CCPA did not come into effect until January 1, 2020, nearly a year after Plaintiff filed this action.

ARGUMENT

I. PLAINTIFF'S UCL "FRAUD" PRONG CLAIM FAILS

A. Plaintiff Cannot Prove A "Failure to Disclose" Given That Defendants Disclosed The Allegedly Omitted Information In Their Privacy Policy

Plaintiff does not contend that the TWC App's Android or iOS permission prompts contained *affirmative* misrepresentations. The Android prompt did not contain *any* representations about the uses of location data, and the iOS prompt accurately represented that users who shared their location data would "get personalized local weather data, alerts and forecasts." UF ¶¶ 34, 37.

Rather, Plaintiff contends that, in the permission prompts, Defendants *failed to disclose* their use and sharing of location data for advertising or commercial purposes. Ex. 1 (Compl.) ¶¶ 7, 45-46.

In order to establish a "failure-to-disclose" claim under the UCL's "fraud" prong, Plaintiff must show that Defendants had an affirmative duty to disclose the allegedly omitted information. *Berryman v. Merit Prop. Mgmt., Inc.*, 152 Cal. App. 4th 1544, 1556-57 (4th Dist. 2007) ("Absent a duty to disclose, the failure to do so does not support a claim under the fraudulent prong of the UCL."); *O'Shea v. Epson Am., Inc.*, 2011 WL 3299936, at *6 (C.D. Cal. July 29, 2011) ("Here, because there is no allegation that the 'omitted' information was contrary to an actual representation, to defeat summary judgment and prevail on an omission-based theory of liability, Plaintiffs must establish that [defendant] was affirmatively obligated to disclose the information."), *aff'd*, 566 F. App'x 605 (9th Cir. 2014).

A defendant has a duty to disclose only in four limited situations: "(1) when a defendant is in a fiduciary relationship with plaintiff; (2) when a defendant had exclusive knowledge of material facts not known to plaintiff; (3) when a defendant actively conceals a material fact from plaintiff; or (4) when a defendant makes partial representations but also suppresses some material facts." *Rubenstein v. The Gap, Inc.*, 14 Cal. App. 5th 870, 877 (2d Dist. 2017). None of these circumstances is present here. Plaintiff does not allege there is any fiduciary relationship between Defendants and App users. Defendants did not have "exclusive knowledge" of the fact that users' location data would be used and shared for advertising, nor did Defendants "actively conceal" or "suppress" this fact—they disclosed it in their Privacy Policy. UF ¶ 21.

Plaintiff will likely argue that Defendants made a misleading "partial representation" because the permission prompts did not disclose the use and sharing of location data for advertising. This theory plainly fails with respect to the Android prompt because that prompt (for which Google supplied the text) did not list *any* data use purposes—it merely asked for permission to access the device's location data. UF ¶¶ 34, 35; Ex. 12. *See Belton v. Comcast Cable Holdings, LLC*, 151 Cal. App. 4th 1224, 1241 (1st Dist. 2007) (where defendant represented that a "subscription to basic cable 'is required'" for other services, holding that no reasonable user would "infer from the mere *absence* of any stated reason" that such subscription was necessary for legal or technical reasons).

Plaintiff thus cannot rely on a "partial representation" theory as to Android users.

As for iOS users, Plaintiff's "partial representation" theory fails because Defendants provided reasonable notice that they may use and share users' location data for advertising in their Privacy Policy. The UCL requires only "reasonable" notice, not "the best possible notice," and it was clearly "reasonable" for Defendants to disclose their use and sharing of location data for advertising in their Privacy Policy, where the Legislature determined such disclosures *should* be made. *See, e.g.*, *Nolte v. Cedars-Sinai Med. Ctr.*, 236 Cal. App. 4th 1401, 1409 (2d Dist. 2015) (affirming dismissal of UCL claim based on allegation that hospital did not sufficiently disclose its billing practices because hospital complied with applicable regulations; allegation that hospital "did not separately and specifically disclose and explain" its practices beyond what regulations required was insufficient to state a UCL "fraud" prong claim); *Plotkin v. Sajahtera, Inc.*, 106 Cal. App. 4th 953, 965-66 (2d Dist. 2003) (affirming dismissal of UCL claim where plaintiff alleged defendant hotel should have made disclosure in a sign, rather than a parking ticket); *Maloney v. Verizon Internet Servs., Inc.*, 2009 WL 8129871, at *5 (C.D. Cal. Oct. 4, 2009) (dismissing UCL fraud claim based on representation that internet speed was "up to 3 Mbps," where terms of service explained that internet speed might actually be less than "3 Mbps").

Moreover, a review of the Privacy Policy would have "dispelled" any possible ambiguity that a user "would read into" the permissions prompt, so Defendants had no duty to make additional just-in-time disclosures. *See Freeman v. Time, Inc.*, 68 F.3d 285, 290 (9th Cir. 1995) (plaintiff failed to state a claim under UCL because "[a]ny ambiguity that [plaintiff] would read into any particular statement is dispelled by the promotion as a whole"). Given that CalOPPA requires the information at issue to be disclosed in a Privacy Policy, that is exactly where reasonable consumers would expect to find it. Until CCPA became effective on January 1, 2020—nearly a year after Plaintiff filed suit—consumers would have had no reason to expect such information to be disclosed anywhere else, such as in the "just-in-time notice" or "pop-up" that Plaintiff now asserts was necessary.

B. Plaintiff Cannot Prove That The Allegedly Omitted Information Was Material

Plaintiff's fraud claim fails for the independent reason that Plaintiff cannot show that the allegedly omitted information was "material." *See Rubenstein*, 14 Cal. App. 5th at 878 (no duty to

disclose absent a showing that the omitted information was "material to reasonable consumers"). Under the UCL, "[m]ateriality exists if the omitted information would cause a reasonable consumer to behave differently if he or she were aware of it." *O'Shea*, 2011 WL 3299936, at *6; *see also Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 332-33 (2011) ("A misrepresentation is judged to be 'material' if a reasonable man would attach importance to its existence or nonexistence *in determining his choice of action in the transaction in question*") (emphasis added).

For Plaintiff to prove materiality here, he would have to show that Defendants' specific disclosure of their use and sharing of location data for advertising in their January 24, 2019 revised iOS permission prompt and the April 24, 2019 Android and iOS Blue Screens caused a substantial *decrease* in the rates at which users shared their location data with the App. But, as Dr. Snow's analysis demonstrates, the Sessions Data shows that users continued sharing their location data with the App at approximately the same rate even after being specifically alerted to the allegedly omitted information and clicking "I Understand." UF ¶ 47; Ex. 23 (Snow Rept.), ¶¶ 23, 35-53.

The Sessions Data thus confirms that Defendants' use and sharing of location data for advertising was either (a) irrelevant to users' decisions to share their location with the App, or (b) consistent with assumptions or expectations that users already held. *See Daugherty v. American Honda Motor Co., Inc.*, 144 Cal. App. 4th 824, 838 (2d Dist. 2006), *as modified* (Nov. 8, 2006) (defendant's omission that engine defect might eventually cause oil leak was not "likely to deceive the general public" because the "only expectation buyers could have had" about the engine was that it would function properly for the length of the warranty); *Bardin v. DaimlerChrysler Corp.*, 136 Cal. App. 4th 1255, 1275 (4th Dist. 2006) (rejecting claim under UCL fraud prong because, "[i]n order to be deceived, members of the public must have had an expectation or an assumption about the materials used" in the vehicle, and the plaintiff alleged no such expectation); *Buller v. Sutter Health*, 160 Cal. App. 4th 981, 988 (1st Dist. 2008) (failure to disclose discount policy was not likely to deceive consumers where they were "not likely to be operating under the expectation that they are entitled to a discount"). Plaintiff cannot prove materiality under either scenario, and therefore his "fraud" claim should be dismissed.

II. PLAINTIFF'S UCL "UNFAIR" PRONG CLAIM FAILS

"In consumer cases arising under the UCL, a business practice is 'unfair' if (1) the consumer injury is substantial; (2) the injury is not outweighed by any countervailing benefits to consumers or competition; and (3) the injury could not reasonably have been avoided by consumers themselves." *Klein v. Chevron U.S.A., Inc.*, 202 Cal. App. 4th 1342, 1376 (2d Dist. 2012) (citing *Camacho v. Auto. Club of So. Cal.*, 142 Cal. App. 4th 1394, 1403 (2d Dist. 2006)).[6]

A. Plaintiff Cannot Prove That TWC App Users Suffered A Substantial Injury

Plaintiff's "unfair" prong claim fails because Plaintiff cannot establish any cognizable consumer injury, let alone a "substantial" injury. *See Klein*, 202 Cal. App. 4th at 1376. This is because: (1) Plaintiff alleges only speculative emotional harms, which are not "substantial injuries" as a matter of law, particularly in light of the fact that many consumers benefited from TWC's use of their location data; and (2) even if subjective, emotional harms constituted "substantial injuries" (they do not), Defendants' alleged failure to disclose the ways in which they used consumers' location data was not the cause of any such harm.

1. Speculative, Emotional Harms Are Not "Substantial Injuries"

Plaintiff "[a]dmit[s] that some users of the TWC App would consider receiving tailored advertising on the TWC App based on their current location or location history *to be a benefit, not a harm*." Ex. 3 (Plaintiff's Responses and Objections to IBM's First Set of Requests for Admission, Response to RFA No. 2) at AE 68 (emphasis added); UF ¶ 18. An injury cannot be "substantial" where, as here, it indisputably benefits some consumers. *See Puentes v. Wells Fargo Home Mortg., Inc.*, 160 Cal. App. 4th 638, 648-49 (4th Dist. 2008) (lender's method of calculating interest did not cause "substantial" injury, even though it resulted in overcharges for some consumers, where the "practice benefited many consumers"); *see also In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 987-89 (N.D. Cal. 2014) (dismissing UCL claim because the "benefit to users in receiving

[6] Although "[t]here is currently a split of authority with respect to the proper definition of the term 'unfair' in the context of consumer cases arising under the UCL . . . [the Second] district has consistently followed the definition enunciated in *Camacho*, which was decided by Division Eight of this district in 2006." *Klein*, 202 Cal. App. 4th at 1376 n.14 (citation omitted).

free, 'indispensable services' offsets much of the harm they may suffer" from the disclosure of their data).

That is all the more true because Plaintiff cannot identify a concrete injury suffered by users, such as a monetary loss, that could be weighed against the benefits users receive by sharing their location data. As Plaintiff admits, "[t]he [alleged] injury is mental and subjective." Ex. 2 (Plaintiff's Rog Responses, Response No. 11) at AE 55; *id.* (Response No. 7) at AE 52 (noting courts weigh "countervailing benefits" against alleged harms). No court has held that a "mental and subjective" injury constitutes a "substantial injury" under the UCL, and the relevant authorities squarely reject that theory.

As a leading treatise on California's UCL (the Rutter Guide) explains: "Trivial or speculative harm is insufficient, and must arise to real monetary harm or unwarranted health and safety risks. Likewise, *emotional harm will not render a practice unfair*." Cal Prac. Guide, "Unfair" Business Practices, Bus. & Prof. C. 17200, Ch. 3-G § 3:126 (emphasis added). The Rutter Guide reached this conclusion based on an extensive survey of case law interpreting Section 5 of the Federal Trade Commission ("FTC") Act, which similarly prohibits "unfair" conduct, and to which California courts turn for guidance in determining the scope of the UCL's "unfair" prong. *Id.* § 3:122 ("Since the [California] Supreme Court has decided that the test of 'unfair' may borrow from the FTC's test, it is therefore useful to examine what 'unfair' means in consumer cases brought by the FTC for violations of § 5 of the FTC Act."); *see also Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 185 (1999) (explaining that the UCL and section 5 of the FTC Act are "parallel" statutes and concluding that "[i]n view of the similarity of language and obvious identity of purpose of the two statutes, decisions of the federal court on the subject are more than ordinarily persuasive").[7]

[7] *See also Camacho*, 142 Cal. App. 4th at 1403 (California courts "may turn for guidance to the jurisprudence arising under section 5 of the Federal Trade Commission Act") (citation and internal quotes omitted); *In re Firearm Cases*, 126 Cal. App. 4th 959, 980 (1st Dist. 2005) ("We follow the lead of the *Cel-Tech* court in consulting parallel federal authority to assist in determining the appropriate reach of the UCL.").

Confirming that Plaintiff alleges only subjective, emotional injuries, Plaintiff identified *only* the following injuries in response to Defendants' interrogatories on this subject:

- "Users' loss of control over sensitive, personal location data without being provided material information about how that data is used, to whom it is shared, and how it is stored and maintained—and without receiving adequate compensation in exchange; [¶]
- the *risk* of misuse of users' location data by Defendants and/or other third parties with whom such data is shared, including but not limited to the use of such data to discover the identity of users, to learn intimate details about users' whereabouts, and to follow and/or stalk users; [¶]
- the aggregation of users' location data with other personal data in ways that users would not reasonably expect and that further intrude upon users' privacy; and [¶]
- harms associated with the *risk* of further unauthorized disclosure of users' location data through breaches or hacks of TWC and/or other third parties with whom such data is shared."

Ex. 2 (Plaintiff's Rog Responses, Response No. 11) at AE 54-55 (emphasis added).

These types of intangible, subjective injuries are foreclosed by the case law because courts must weigh the costs and benefits of a given practice in order to determine whether it is "unfair," and that analysis is impossible when only subjective harms are at issue. *See Cel-Tech*, 20 Cal. 4th at 166 (in determining whether conduct is "unfair" under the UCL, "courts may not apply purely subjective notions of fairness"); *LabMD, Inc. v. FTC*, 678 F. App'x 816, 820-21 (11th Cir. 2016) (in case under the FTC Act, explaining that intangible harms are generally not actionable, particularly where they are "only speculative"; concluding that *potential* data breach was likely not a substantial injury because it resulted in only "intangible harms"); *FTC v. Alcoholism Cure Corp.*, 2011 WL 13137951, at *53 (M.D. Fla. Sept. 16, 2011) ("In most cases 'substantial injury' involves monetary harm."), *aff'd sub nom. FTC v. Krotzer*, 2013 WL 7860383 (11th Cir. May 3, 2013); *see also* S. REP. 103-130, 13, 1993 WL 322671 (legislative history on FTC's section 5 test) ("[S]ubstantial injury is not intended to encompass merely trivial or speculative harm. In most cases, substantial injury would involve monetary or economic harm or unwarranted health and safety risks. Emotional impact and more subjective types of harm alone are not intended to make an injury unfair.").

Here, in particular, the Court should be skeptical of treating the alleged "mental and subjective" injuries as "substantial" injuries because there is no evidence that any significant

population of consumers believe they are meaningfully harmed by the use or sharing of their location data for advertising. To the contrary, as Dr. Snow explains, the Sessions Data shows that consumers continued to share their location data with the TWC App at the same rate even after Defendants specifically apprised them of Defendants' use and sharing of their location data and required them to click "I Understand." UF ¶ 47; Ex. 23 (Snow Rept.) ¶¶ 23, 35-53. The Sessions Data is thus quantifiable proof that *most* users do not consider Defendants' use and sharing of location data for advertising to be an "injury" *at all*, let alone a "substantial" one.

Plaintiff's remaining "injury" arguments also fail. Plaintiff asserts that some users may feel they have not received "adequate compensation" for their location data. Ex. 2 (Plaintiff's Rog Responses, Response No. 11) at AE 54-55. Even if there were evidence supporting this assertion (there is not), any such subjective belief does not amount to a "substantial injury" because Plaintiff has not alleged that users have a property interest in their location data. Ex. 2 (Plaintiff's Rog Responses, Response No. 10) at AE 53-54 (Plaintiff does not contend "that users of the TWC App have a property interest in the data Defendants collect through the app."). If users have no property interest in their location data, Defendants' alleged failure to compensate them for it does not constitute an injury.[8] *See Rojas-Lozano v. Google, Inc.*, 159 F. Supp. 3d 1101, 1117-18 (N.D. Cal. 2016) (it was not "unfair" under the UCL for Google to profit off users' transcriptions of words without their knowledge when users received a free email account in exchange and plaintiff "failed to identify any statute assigning value to the few seconds it takes to transcribe one word").

Plaintiff also speculates that location data could be misused to "stalk" users. Even if this were possible, notwithstanding the facts that Defendants generally do not collect personal identifying information about users and employ numerous safeguards to prevent the identification of users based on their location data, there is no evidence that location data has ever been misused

[8] Indeed, if this case had been brought by users themselves rather than the City Attorney, the users would not even have standing to pursue it because they have not "lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204; *see Archer v. United Rentals, Inc.*, 195 Cal. App. 4th 807, 815-16 (2d Dist. 2011) (plaintiffs lacked standing where they claimed that "the unfair business practice is the unlawful collection and recordation of their personal identification information," because they failed to demonstrate a loss of money or property).

in this manner. UF ¶¶ 27, 29. Plaintiff similarly professes concern regarding "breaches or hacks of TWC and/or other third parties with whom such data is shared." But, again, there is no evidence that users' location data has ever been the subject of any "breach" or "hack." UF ¶ 33. These are purely hypothetical injuries, not "substantial" ones. *See LabMD*, 678 F. App'x at 821 (in FTC Act case, holding that potential unauthorized disclosure by medical lab of names, birthdates, addresses, social security numbers, and medical and insurance information for 9,300 patients likely did not constitute a substantial injury "because this harm is only speculative").

Finally, Plaintiff speculates that Defendants may "aggregat[e] users' location data with other personal data in ways that users would not reasonably expect." Ex. 2 (Plaintiff's Rog Responses, Response No. 10) at AE 56. This vague assertion is difficult to evaluate given that (1) Plaintiff does not identify the "other personal data" that might be "aggregated" with location data in a purportedly injurious way, and (2) Defendants generally do not collect personal identifying information such as names, contact information, or credit card numbers from TWC App users. UF ¶¶ 27-28. In any event, even if Plaintiff's speculation were correct, the mere aggregation of location data with (unspecified) "other personal data," without more, is insufficient to establish a "substantial injury." *See In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *15 (N.D. Cal. Dec. 3, 2013) (allegations of Google commingling user data did not state a claim under the UCL's "unfair" prong or for intrusion upon seclusion).

In short, Plaintiff asks the Court to endorse a sweeping and unprecedented expansion of the UCL. It is undisputed that some consumers would view receiving location-tailored advertising as a "benefit"; there is statistical evidence showing that *most* users *choose* to share their location data with the TWC App, even after Defendants' use and sharing of that data for advertising purposes is specifically disclosed in a permission prompt or Blue Screen; and there is *no* evidence that a single user suffered any concrete injury. No court has ever found "substantial injury" on similar facts, and this Court should not be the first to do so.

2. Plaintiff Cannot Establish Causation

Even assuming Plaintiff could prove that the injuries alleged constitute "substantial injuries" (he cannot), Plaintiff's "unfair" prong claim fails because Defendants' alleged failure to disclose

their uses of location data in the location-access permission prompt did not *cause* any such injury. A plaintiff must "show some connection between conduct by defendants and the alleged harm to the public. . . . Without evidence of a causative link between the unfair act and the injuries or damages, unfairness by itself merely exists as a will-o'-the-wisp legal principle." *Firearm Cases*, 126 Cal. App. 4th at 978.

Here, the allegedly unfair practice (the lack of disclosure in the permission prompt that location data would be used and shared for advertising) cannot have caused any injury given that the Sessions Data shows users made the same choice when the allegedly omitted information *was* disclosed in the permission prompt and Blue Screen. UF ¶¶ 47-53; Ex. 23 (Snow Rept.) ¶¶ 25, 35-53; *see also Fabozzi v. StubHub, Inc.*, 2012 WL 506330, at *7 (N.D. Cal. Feb. 15, 2012) (dismissing UCL claim for lack of causation where "it is difficult to see how omitting information [] could have caused the harm Plaintiff alleges"). Because Defendants' allegedly inadequate disclosures are "not connected to [consumers'] harm by causative evidence," Plaintiff's "unfair" prong claim fails. *Firearm Cases*, 126 Cal. App. 4th at 981 ("The UCL provisions are not so elastic as to stretch the imposition of liability to conduct that is not connected to the harm by causative evidence.").

B. TWC App Users Could Reasonably Have Avoided Any Purported Injury

For a business practice to be unfair, the injury must not only be substantial, it must also be one that "could not reasonably have been avoided by consumers themselves." *Klein*, 202 Cal. App. 4th at 1376. Here, consumers could easily have avoided any alleged injury by reviewing the TWC App's Privacy Policy or choosing not to share their device's location data. UF ¶ 26.

Importantly, because Plaintiff has admitted that some users would consider Defendants' use and sharing of location data to deliver more relevant ads a "benefit," UF ¶ 18, the only consumers who were even arguably "injured" are those who are particularly sensitive to privacy concerns. For those consumers, the most *obvious* place to look for information about how their location data might be used was in the Privacy Policy, which specifically disclosed the allegedly omitted information. *See Lavie v. Procter & Gamble Co.*, 105 Cal. App. 4th 496, 512 (1st Dist. 2003) (standard in UCL cases is whether a consumer acted "reasonably under the circumstances"). Any reasonable consumer who read the Privacy Policy would therefore know that their location data might be used

and shared for advertising, and could have prevented that by declining to give the App access to their device's location data.[9] *See Camacho*, 142 Cal. App. 4th at 1406 (plaintiff could reasonably have avoided the injury by obtaining insurance); *Davis v. Ford Motor Credit Co. LLC*, 179 Cal. App. 4th 581, 598 (2d Dist. 2009) (alleged injury of late fees was reasonably avoidable because the fees could have been avoided if plaintiff made payments on time).

Plaintiff may argue that consumers could not have avoided sharing their location data because Defendants "buried" these disclosures in the Privacy Policy to ensure that consumers never read them. *See* Ex. 1 (Compl.) ¶¶ 30-34. But Defendants disclosed in the Privacy Policy because that is where the Legislature determined the information *should* be disclosed. According to the Legislature, CalOPPA "*provides meaningful privacy protections . . . by allowing individuals to rely on a privacy policy posted online*." Ex. 4 (Assem. Com. on Judiciary Analysis) at AE 75 (emphasis added). That is, the Legislature concluded that it is reasonable for consumers to "rely on" a privacy policy such as the one Defendants maintained in order to determine how their personal information is being used. *Id.* Any argument that it was somehow "unfair" for Defendants to disclose this information in the Privacy Policy is meritless.

Plaintiff may also argue that it was too difficult for consumers to review Defendants' Privacy Policy—because, for example, it allegedly was too long. Ex. 1 (Compl.) ¶ 7. Even a cursory glance at the Privacy Policy in effect at the time Plaintiff filed suit makes clear that it is written in plain English, not legal jargon, and is easy to navigate, with a hyperlinked table of contents on the first page that takes users to the relevant sections. *See* Ex. 13.

In any event, it is not "unfair" for consumers to have to undertake minimal efforts to seek out information that is important to them. In *Hodsdon v. Mars, Inc.*, 162 F. Supp. 3d 1016, 1024-27 (N.D. Cal. 2016), *aff'd*, 891 F.3d 857 (9th Cir. 2018), for example, the defendant failed to disclose that its candy bars were made using a supply chain that involved forced child labor—a fact reasonable consumers might find extremely problematic. The court nonetheless dismissed the

[9] *See* Ex. 1 (Compl.) ¶ 35 (alleging that approximately 20% of users decline to grant access to their device's location data). These users avoided any alleged "injury," confirming that all users could reasonably have avoided the injury in this same manner.

plaintiff's UCL claim because the relevant information was "readily available to consumers on [defendant's] website." *Id.*; *see also Rubenstein*, 14 Cal. App. 5th at 880 (in case involving alleged failure to disclose differences between clothing types, finding no unfair business practice because "[a] consumer who cared about" such differences "could have asked a sales associate"). Similarly, here, "the fact is that [consumers] could have avoided any and all" alleged injury simply by taking a few minutes to review Defendants' Privacy Policy. *Camacho*, 142 Cal. App. 4th at 1406.

CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court grant their motion for summary judgment and dismiss Plaintiff's UCL claim with prejudice.

DATED: June 11, 2020

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By /s/ *Stephen A. Broome*
James R. Asperger
Stephen A. Broome
Lauren B. Lindsay
William R. Sears

Attorneys for Defendants
TWC PRODUCT AND TECHNOLOGY, LLC
INTERNATIONAL BUSINESS MACHINES CORPORATION

PROOF OF SERVICE

STATE OF CALIFORNIA, COUNTY OF LOS ANGELES

At the time of service, I was over 18 years of age and not a party to this action. I am employed in the County of Los Angeles, State of California. My business address is 865 South Figueroa Street, 10th Floor, Los Angeles, CA 90017-2543.

On June 11, 2020, I served true copies of the following document(s) described as **DEFENDANTS' NOTICE OF MOTION AND MOTION FOR SUMMARY JUDGMENT ON PLAINTIFF'S UCL CAUSE OF ACTION** on the interested parties in this action as follows:

OFFICE OF THE LOS ANGELES CITY ATTORNEY
Michael N. Feuer
Michael J. Bostrom
Adam R. Teitelbaum
adam.teitelbaum@lacity.org
200 North Spring Street, 14th Floor
Los Angeles, CA 90012-4131

Attorneys for Plaintiff

BY E-MAIL OR ELECTRONIC TRANSMISSION: Based on a court order or an agreement of the parties to accept service by e-mail or electronic transmission, I caused the document(s) to be sent from e-mail address laurenlindsay@quinnemanuel.com to the persons at the e-mail addresses listed in the Service List. I did not receive, within a reasonable time after the transmission, any electronic message or other indication that the transmission was unsuccessful.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on June 11, 2020, at Los Angeles, California.

/s/ Lauren Lindsay
Lauren Lindsay