Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of X-Mode Social, Inc.*, File No. 2123038**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from X-Mode Social, Inc. and Outlogic, LLC (collectively "X-Mode").

The proposed consent order ("Proposed Order") has been placed on the public record for 30 days for receipt of public comments by interested persons. Comments received during this period will become part of the public record. After 30 days, the Commission will again review the agreement, along with the comments received, and will decide whether it should make final the Proposed Order or withdraw from the agreement and take appropriate action.

Respondent X-Mode is a Delaware corporation with its headquarters in Virginia. Respondent Outlogic is a Virginia limited liability company and is the successor-in-interest to Respondent X-Mode. X-Mode is a data broker that collects or purchases precise geolocation data about consumers' mobile devices.

X-Mode occupies multiple roles in the location data marketplace. X-Mode created a Software Development Kit ("SDK") for use in third-party apps, obtained location data from other aggregators, and previously published its own apps "Drunk Mode" and "Walk Against Humanity." X-Mode ingests billions of location signals daily from its various sources. X-Mode sells this location data to marketers, retailers, research organizations, private government contractors for national security, and other data brokers.

X-Mode creates and sells two primary data products: 1) Data-as-a-Service ("DaaS") product, which is raw location data without any additional analysis, consisting of, among other information, a unique persistent identifier for the mobile device called a Mobile Advertiser ID ("MAID") and timestamped latitude and longitude coordinates; and 2) "Audience Segments," which are groupings of MAIDs that purportedly share similar traits based on the locations or events the mobile devices and MAIDs have visited.

The Commission's proposed seven-count complaint alleges that Respondents violated Section 5(a) of the FTC Act by (1) unfairly selling sensitive data, (2) unfairly failing to honor consumers' privacy choices, (3) unfairly collecting and using consumer location data, (4) unfairly collecting and using consumer location data without consent verification, (5) unfairly categorizing consumers based on sensitive characteristics for marketing purposes, (6) deceptively failing to disclose use of location data, and (7) providing the means and instrumentalities to engage in deceptive acts or practices.

With respect to the first count, the proposed complaint alleges that Respondents sold location data associated with MAIDs that could be used to track consumers to sensitive locations, such as medical facilities, places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, and welfare and homeless shelters. For example, by plotting the latitude and longitude coordinates included in the X-Mode data stream using publicly available map programs, it is possible to identify which consumers' mobile devices visited medical facilities and when.

With respect to the second count, the proposed complaint alleges that X-Mode failed, between June 2018 and July 2020, to honor the privacy choices of some consumers who had enabled the "Opt out of Ads Personalization" control on their Android mobile phones. X-Mode's consumers were unaware that their privacy choices were not being honored by X-Mode and the company failed to employ the necessary technical safeguards and oversight to ensure that consumers' privacy choices were honored. The proposed complaint alleges that this failure caused or was likely to cause substantial injury by failing to honor the privacy decisions made by the consumers.

With respect to the third count, the proposed complaint alleges that X-Mode failed to notify users of its own apps (Drunk Mode and Walk Against Humanity) the purposes for which their location data would be used. As a result, the proposed complaint alleges that X-Mode caused or was likely to cause consumers substantial injury by collecting and selling the consumers' sensitive data without consumers' consent.

With respect to the fourth count, the proposed complaint alleges that X-Mode failed to verify that third-party apps incorporating its SDK obtain informed consent from consumers to have the consumers' location data collected, used, and sold. X-Mode's primary mechanism for ensuring that consumers have provided appropriate consent is through contractual requirements with its suppliers. However, contractual provisions, without additional safeguards, are insufficient to protect consumers' privacy.

With respect to the fifth count, the proposed complaint alleges that it was an unfair practice for X-Mode to categorize consumers based on sensitive characteristics. X-Mode entered into an agreement with a privately held clinical research company to trace consumers in Ohio within a 200-meter radius of Cardiologist offices, Gastroenterologist offices, Endocrinologist offices, Pharmacies, and Drugstores. X-Mode licensed these segments for advertising or marketing purposes.

With respect to the sixth count, the proposed complaint alleges that X-Mode represented to users of the X-Mode apps that their data would be used for certain purposes, but failed to disclose it would be provided to government contractors for national security purposes. Such a failure to disclose is material to consumers and is likely to mislead consumers who have no way of determining the truth. As a result, this conduct is deceptive under Section 5.

With respect to the seventh count, the proposed complaint alleges that X-Mode has furnished third party app publishers with language for consumer disclosures that mislead consumers about the purposes for which their location may be used, such as by failing to disclose that consumer's location would be provided to government contractors for national security purposes. Furnishing such materials provided the means and instrumentalities by which the app publishers could mislead consumers and is therefore deceptive under Section 5 of the FTC Act.

The proposed complaint alleges that Respondents could have addressed each of these failures by implementing certain safeguards at a reasonable cost and expenditure of resources.

The proposed complaint alleges that X-Mode's practices caused, or are likely to cause, substantial injury to consumers that are not outweighed by countervailing benefits to consumers

or competition and are not reasonably avoidable by consumers themselves. Such practices constitute unfair acts or practices under Section 5 of the FTC Act.

Summary of Proposed Order with Respondent

The Proposed Order contains injunctive relief designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

Part I prohibits Respondents from misrepresenting the extent to which (1) it collects, maintains, uses, discloses, deletes any covered information, and (2) the location data that Respondents collect, use, maintain, or disclose is deidentified.

Part II prohibits Respondents from selling, licensing, transferring, sharing, disclosing, or using sensitive location data in any products or services.

Sensitive locations are defined as those locations in the United States associated with (1) medical facilities (e.g., family planning centers, general medical and surgical hospitals, offices of physicians, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, outpatient care centers, psychiatric and substance abuse hospitals, and specialty hospitals); (2) religious organizations; (3) correctional facilities; (4) labor union offices; (5) locations of entities held out to the public as predominantly providing education or childcare services to minors; (6) associations held out to the public as predominantly providing services based on racial or ethnic origin; or (7) locations held out to the public as providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants.

Part III requires that Respondents implement and maintain a sensitive location data Program to develop a comprehensive list of sensitive locations and to prevent the use, sale, license, transfer, or disclosure of sensitive location data.

Part IV requires that Respondents establish and implement policies, procedures, and technical measures designed to prevent recipients of Respondents' location data from associating consumers with locations predominantly providing services to LGBTQ+ individuals, locations of public gatherings of individuals during social demonstrations, marches, or protests, or using location data to determine the identity or location of an individual's home.

Part V requires Respondents to notify the Commission any time it determines that a third party shared Respondents' Location Data, in violation of a contractual requirement between Respondents and the third party.

Part VI requires that Respondents must not collect, use, maintain, and disclose location data (1) when consumers have opted-out, or otherwise declined targeted advertising, (2) without a record documenting the consumer's consent obtained prior to the collection of location data, and (3) in connection with Respondents' apps unless consumers receive a clear and conspicuous quarterly reminder about location data being collected.

Part VII requires that Respondents implement a supplier assessment program designed to ensure that consumers have provided consent for the collection and use of location data obtained by Respondents. Under this program, Respondents must conduct initial assessments of all their data suppliers within 30 days of entering into a data sharing agreement, or within 30 days of the initial date of data collection. The program also requires that Respondents confirm that consumers provide consent and create and maintain records of suppliers' assessment responses. Finally, Respondents must cease from using, selling, or disclosing location data for which consumers have not provided consent.

Part VIII requires that Respondents provide a clear and conspicuous means for consumers to request the identity of any entity, business, or individual to whom their location data has been sold, transferred, licensed, or otherwise disclosed or a method to delete the consumers' location data from the databases of Respondents' customers. Respondents must also provide written confirmation to consumers that the deletion requests have been sent to Respondents' customers.

Part IX requires that Respondents provide a simple, easily-located means for consumers to withdraw any consent provided and **Part X** requires that Respondents cease collecting location data within 15 days after Respondents receive notice that the consumer withdraws their consent.

Part XI also requires that Respondents provide a simple, easily-located means for consumers to request that Respondents delete location data that Respondents previously collected and to delete the location data within 30 days of receipt of such request unless a shorter period for deletion is required by law.

Part XII requires that Respondents (1) document and adhere to a retention schedule for the covered information it collects from consumers, including the purposes for which it collects such information, the specific business needs, and an established timeframe for its deletion, and (2) prior to collecting or using new type of information related to consumers that was not previously collected, and is not described in its retention schedule, Respondents must update its retention schedule.

Part XIII requires that Respondents delete or destroy all historic location data and all data products. Respondents have the option to retain historic location data if it has obtained affirmative express consent or it ensures that the historic location data is deidentified or rendered non-sensitive. Respondents must inform all customers that received location data from Respondents within 3 years prior to the issuance date of this Order, of the Commission's position that such data should be deleted, deidentified, or rendered non-sensitive.

Part XIV requires Respondents to establish and implement, and thereafter maintain, a comprehensive privacy program that protects the privacy of consumers' personal information.

Parts XV-XVIII are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide information or documents necessary for the Commission to monitor compliance.

Part XIX states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the Proposed Order, and it is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify the Proposed Order's terms in any way.