Andrew Ferguson

In the Matter of Gravy Analytics, Inc., a corporation, and Venntel, Inc., acorporation.	DECISION AND ORDER Docket No. C-____

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondents that

The Commission considered the matter and determined that it had reason to believe

Findings

The Respondents are:

a. Respondent Gravy Analytics, Inc., a Delaware corporation with its principal office or place of business at 44679 Endicott Dr Suite 300, Ashburn, VA 20147.

b. Respondent Venntel, Inc., a Delaware corporation with its principal office or place of business at 2201 Cooperative Way, Suite 600, Herndon, Virginia 20171. Venntel is a wholly-owned subsidiary of Gravy Analytics.

The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

ORDER

Definitions

For the purpose of this Order, the following definitions apply:

A. "Affirmative Express Consent" means any freely given, specific, informed, and unambiguous indication of an individual consumer's wishes demonstrating agreement by the individual, such as by an affirmative action, following a Clear and Conspicuous Disclosure to the individual of: (1) the categories of information that will be collected; (2) the purpose(s) for wheoeonfor wheo(r)-2 (a3 (ot)-th)28Re whecaon oduagr l o: 2or/TTEMC /LE

2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

C. "Covered Information" means information from or about an individual consumer including, but not limited to: (1) a first and last name; (2) Location Data; (3) an email address or other online contact information; (4) a telephone number; (5) a Social Security number; (6) a driver's license or other government-issued identification number; (7) a financial institution account number; (8) credit or debit card information; (9) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; or (10) socioeconomic or demographic data. Deidentified information is not Covered Information.

D. "Data Product" means any model, algorithm, or derived data, in Respondents' custody or control, developed, in whole or part, using Historic Location Data. Data Product includes but is not limited to any derived data produced via inference (manual or automated) or predictions such as audience segments.

E. "Deidentified" or "Deidentifiable" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular person, in that Respondents must, at a minimum:

1. Have implemented technical safeguards that prohibit reidentification of the person to whom the information may pertain;

2. Have implemented business processes that specifically prohibit reidentification of the information, including by buyers, customers, or other entities to whom Respondents provide the information;

3. Have implemented business processes to prevent inadvertent release of Deidentified information; and

4. Make no attempt to reidentify the information.

F. "Historic Location Data" means any Location Data that Respondents collected from consumers without consumers' Affirmative Express Consent.

G. "Location Data" means any data that may reveal a mobile device's or consumer's precise location, including but not limited to Global Positioning System (GPS) coordinates, cell tower information, or precise location information inferred from basic service set identifiers (BSSIDs), WiFi Service Set Identifiers (SSID) information, or Bluetooth receiver information, and any unique persistent identifier combined with any such data, such as a mobile advertising identifier (MAID) or identifier for advertisers (IDFA). Data that: (1) reveals only a mobile device or consumer's coarse location data (e.g., zip code or census block location with a radius of at least 1,850 feet), or (2) is used for (a) Security Purposes, (b) National Security purposes conducted by federal agencies or other federal entities, or (c) response by a federal law enforcement agency to an imminent risk of death or serious bodily harm to a person, is not Location Data.

H. "National Security" means the national defense, foreign intelligence and counterintelligence, international and internal security, and foreign relations. This includes countering terrorism; combating espionage and economic espionage conducted for the benefit of any foreign government, foreign instrumentality, or foreign agent; enforcing export controls and sanctions; and disrupting cyber threats that are perpetrated by nation states, terrorists, or their agents or proxies.

I. "Raw Format" means the format in which Location Data is originally supplied, prior to any form of processing, extraction, or analysis taking place.

J. "Respondents" means Gravy Analytics, Inc. ("Gravy") and Venntel, Inc. ("Venntel"), and their successors and assigns.

K. "Security Purposes" means preventing, detecting, protecting against, or responding to data security incidents, including cybersecurity incidents, identity theft, fraud, phishing, harassment, malicious or deceptive activities, or preserving the integrity or security of systems.

L. "Sensitive Locations" means locations within 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; (7) locations held out to the public as providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants; or (8) military installations, offices, or buildings.

M. "Sensitive Location Data" means any consumer Location Data associated with a Sensitive Location.

N. "Third-Party Incident" means the sharing by a third party of Respondents' Location Data, in violation of a contractual requirement between Respondents and the third party.

Provisions

I. Prohibition Against Misrepresentations

IT IS ORDERED that Respondents and Respondents' officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, promotion, offering for sale, sale, or distribution of any product or service, must not misrepresent, in any manner, expressly or by implication:

A. The extent to which Respondents review data suppliers' compliance and consent frameworks, consumer disclosures, sample notices, and opt in controls;

B. The extent to which Respondents collect, use, maintain, disclose, or delete any Covered Information; and

C. The extent to which the Location Data that Respondents collect, use, maintain, or disclose is Deidentified.

III. Sensitive Location Data Program

IT IS FURTHER ORDERED that Respondents,

5. Documenting each step of this assessment, including the reasons Respondents selected the methods, sources, products, or services used in updating Respondents' list of Sensitive Locations.

F. Implement policies, procedures, and technical measures designed to prevent Respondents from using, selling, licensing, transferring, or otherwise sharing or disclosing Sensitive Location Data as provided in Provision II above, and monitor and test the effectiveness of these policies, procedures, and technical measures at least once every three months. Such testing must be designed to verify that Respondents are not using, selling, licensing, transferring, or otherwise sharing or disclosing Sensitive Location Data;

G. Initiate the process of deleting or rendering non-sensitive Sensitive Location Data associated with locations included in the list developed pursuant to Subparts D and E, within 2 days of adding the location to the list of Sensitive Locations, and complete the process within 30 days of initiation, except where retention is needed to fulfill an allowed purpose as provided in Provision II above. The time period to complete this process may be extended by additional 30 days periods (not to exceed 90 total days) when reasonably necessary, provided the Respondents document at each interval, the reasons for the extension and the progress made, and Respondents must not use, provide access to, or disclose Sensitive Location Data during the process of deleting or rendering non-sensitive, for any other purpose; and

H. Evaluate and adjust the Sensitive Location Data Program in light of any changes to Respondents' operations or business arrangements, or any other circumstance that Respondents know or have reason to know may have an impact on the Sensitive Location Data Program's effectiveness. At a minimum, Respondents must evaluate the Sensitive Location Data Program every twelve months and implement modifications based on the results.

IV. Other Location Data Obligations

IT IS FURTHER ORDERED that Respondents, within 90 days of the effective date of this Order, must establish and implement and thereafter maintain policies, procedures, and

1. Contractual

Conspicuous means for consumers to request the identity of any entity, business, or individual as to which Respondents have knowledge that consumers' Location Data was sold, transferred, licensed, or otherwise disclosed. Respondents may require consumers to provide Respondents with information reasonably necessary to complete such requests and to verify their identity, but must not use, provide access to, or disclose any information collected for such a request for any other purpose.

, that the Disclosure requirements in this Provision VIII do not apply if Respondents provide consumers with a Clear and Conspicuous method to submit a request to delete their Location Data from the commercial databases of all recipients of such Location Data, expressly instruct (or contractually require) such recipients to honor such requests sent or made available to them by Respondents, expressly request (or contractually demand) written confirmatio-1 (ont)3 (ri (o)]TJ 0)1 (h5n)2 (fir)5 DTa(6.9 h,-1 (2 Tw T* [(fe(n)-2 (t)3 (he)-1 (ponde)-2c -(

Location Data that Respondents previously collected about their mobile device, and delete such Location Data within 30 days of receipt of such request unless a shorter period for deletion is required by law. Respondents shall create and maintain a process by which a deletion request provided to one Respondent is treated as notice to both Respondents. Respondents may require consumers to provide Respondents with information necessary to complete such requests, but must not use, provide access to, or disclose any information collected for a deletion request for any other purpose.

XII. Data Retention Limits

IT IS FURTHER ORDERED that Respondents, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must:

A. Within 60 days of the effective date of this Order, document, adhere to, and make publicly available through a link on the home page of their website(s), in a manner that is Clear and Conspicuous, a retention schedule for Covered Information, setting forth: (1) the purpose or purposes for which each type of Covered Information is collected or used; (2) the specific business needs for retaining each type of Covered Information; and (3) an established timeframe for deletion of each type of Covered Information limited to the time reasonably necessary to fulfill the purpose for which the Covered Information was collected, and in no instance providing for the indefinite retention of any Covered Information;

B. Within 60 days of the effective date of this Order, Respondents shall provide a written statement to the Commission, pursuant to the Provision entitled Comp1 (b)5 (l)-24om 1bu[g

B. Within 90 days after the effective date of this Order, (i) inform Respondents' customers that received Historic Location Data within 3 years prior to the issuance date of this Order, of the FTC's requirement in Provision XIII.A that the FTC requires such data to be deleted, Deidentified, or rendered non-sensitive, and (ii) Respondents shall promptly submit, within 10 days of sending to its customers, all such notices to the Commission under penalty of perjury as specified in the Provision of this Order titled "Compliance Report and Notices"; and

C. Within 90 days after the effective date of this Order, delete or destroy all Data Products, and provide a written statement to the Commission, pursuant to Provision XVI.D, confirming such deletion or destruction.

could be realized and result in the unauthorized collection, maintenance, use, disclosure of, or provision of access to Covered Information.

F. On at least an annual basis, provide privacy training programs for all employees and independent contractors responsible for handling or who have access to Covered

(1) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondents; (2) identify all of the Respondents' businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (4) describe in detail whether and how the Respondents are in compliance with each Provision of this Order, including a discussion of all of the changes the Respondents made to comply -2 (e)-1 (s)-1 (s)-1 .72 13.8 re f 5fomo co