AIRSAGE

February 18, 2011

VIA ELECTRONIC DELIVERY

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: FTC Staff Preliminary Report on Protecting Consumer Privacy - File No. P095416

Dear Secretary Clark:

AirSage, Inc. ("AirSage") submits these comments in response to Staff's request for feedback on its preliminary report on consumer privacy, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" ("Staff Report").

I. Introduction

AirSage, Inc. provides real-time and historical population location, movement, and traffic information derived from analysis of wireless (and in particular, cellular phone) signaling data. AirSage's products include products supporting 911 calls and traffic flow information services used by government agencies for traffic and roadway planning and for disaster and emergency preparedness. AirSage also provides location based services to the mobile industry and others in the form of aggregated and anonymized mobile data and market segmentation services

Given AirSage's unique and deep experience in mobile location services to the government and industry, Airsage welcomes the opportunity to provide input to Staff regarding the unique challenges of aggregated and anonymized location data to help develop a privacy framework that protects consumer data while taking into account the many benefits of mobile data. AirSage addresses Staff's request for input in the area of "Scope" particularly in the area of linkable data and anonymized data as applied to location based services.

II. Benefits of Location Services

The ability to collect mobility data supports many beneficial products and services valuable and vital to the government, society, individuals and industry.

Transportation professionals relied on by federal, state and local government require large volumes of detailed and complex data to help prioritize where to place and upgrade roadways and other critical infrastructure and to address transportation safety and security concerns. Areas where detailed mobility data is vital include evacuation planning and

management, emergency response (E-911), traffic congestion management, and transportation planning and operations.

Wireless carriers also rely on location data to provide a variety of services. Carriers need detailed location data to test, manage and improve networks and coverage. The current rate of industry growth and consumer demand for wireless services will quickly outpace carriers' network capacity without expansion of services. Improving services including knowing where to add cell tower sites is crucial to increasing coverage to respond to this increased consumer demand.

Consumers are increasingly experiencing the benefits of, and demanding more, location based services. GPS Navigation, weather alerts, traffic updates, and locating restaurant, gas and coffee shops rank among the most popular location services used by consumers. According to a recent Pew Research survey, 7 percent of adults who go online with their mobile phone use a location-based service.[1] Those figures are expected to grow. According to a more recent study by Microsoft and Cross-Tab Marketing Services & Telecommunications Research Group,[2] 50 percent of U.S. consumers have used location-based services. Of the consumers using them, 99 percent said they were either very valuable or somewhat valuable. Consumers also prefer free location-based service applications.[3]

The marketplace has responded to this consumer demand with an increased number of free location-based service applications. These mobile applications, though unpaid by the consumer, derive their funding from advertising revenue. Due to this consumer demand, for some mobile platforms, advertising revenue is now larger than the revenue derived from paid applications.[4] Sixty percent of mobile service providers view location-based advertising as a major part of their offerings in the next three years.[5] Because mobile consumers highly value and respond to relevant, timely advertisements about products and services near them, location data is extremely valuable to this advertising ecosystem.

III. "Linkable" Location Data

AirSage takes individual privacy protection very seriously and recognizes the concerns raised by the FTC regarding linkable data particularly in connection with location data. AirSage addresses the following questions staff raises around linkable data:

---

[1] Kathryn Zickuhr & Aaron Smith, *4% of Online Americans Use Location Based Services*, Pew Research Center's Internet & American Life Project (Nov. 4, 2010), http://www.pewinternet.org/~/media//Files/Reports/2010/PIP-Location%20based%20services.pdf.

[2] Location Based Services Usage & Perceptions Survey, *available at* http://www.microsoft.com/privacy/dpd/.

[3] *Id.*

[4] Due to this consumer demand, for some mobile platforms, advertising revenue is now larger than the revenue derived from paid applications.[1] U.S. mobile local advertising is expected to grow nearly ten-fold, from just over $200 million in 2009 to $2.02 billion in 2014. http://www.slideshare.net/pmork/sizing-up-the-global-mobile-apps-market.

[5] [1] Chetan Sharma, Sizing up the Global Mobile Apps Market, http://www.slideshare.net/pmork/sizing-up-the-global-mobile-apps-market

[1] Study says: mobile local advertising to reach $2 billion by 2014, TechJournal South (Sept. 28, 2010), http://www.techjournalsouth.com/2010/09/study-says-mobile-local-advertising-to-reach-2-billion-by-2014/ (citing BIA/Kelsey's U.S. Local Media Forecast (2009-2014)). http://www.alcatel-lucent.com/advertising/docs/Targeted_Interactive_Advertising_WP.pdf

Whether applying the framework to data that can be "reasonably linked to a specific consumer, computer, or other device" is feasible, particularly with respect to data that, while not currently considered "linkable," may become so in the future. If not feasible, what are some alternatives? Are there reliable methods for determining whether a particular data set is linkable or may become linkable?

AirSage respectfully submits that Staff should consider the following in connection with these questions: 1) Not all location data is the same or has the same degree of linkability, 2) Even location data that may be linked can be safeguarded in alternative ways to protect individual privacy obviating the need for full application of the framework, and 3) Full application of the framework to otherwise appropriately safeguarded location data would greatly impact the mobile marketplace, consumer expectations and critical public services.

A. Not All Location Data is Equally "Linkable."

Not all location data is created or used equally. Mobile location data is derived from a variety of sources that have varying degrees of precision. A-GPS data can be very precise, within 10-20 meters of an individual's location, while a cell site generated location can be up to a mile off.[6] Moreover, while location information may be originally sourced from precise location data, in actual use it may be converted to zip code level, city, state or even country location.

B. Location Data Can Be Safeguarded to Prevent Linking.

An alternative way to protect individual user privacy is to put in place heightened safeguards that mitigate this risk of location data possibly being linked to individuals. Staff should consider a company's use of these mitigating safeguard methods as a safe harbor to include in its list of commonly accepted practices.

First, intended use of the data should be considered. If location data is not intended to be linked to individuals and practices are put in place to help ensure this, this should be taken into account. Companies can demonstrate their commitment to this intention by implementing enforceable internal policies and guidelines against linking data or otherwise identifying or targeting individuals. Companies can also ensure that their vendors and third party service providers who need access to the data also agree not to link data or attempt to link data to individuals. AirSage, for example, removes any personally identifiable data from any location data it derives from carriers, pseudonymizes the data solely for the purpose of creating aggregate reports and has strict policies in place prohibiting use of that pseudonymized data to identify or target individuals.

Second, companies can similarly commit to not sharing personally identifiable location data with independent third parties for those third parties' own uses or allowing third parties acting on such companies' behalf to do the same. An example of this is AirSage's own practice of removing any personally identifying information from any data before it leaves the

[6] In tests by Qualcomm, location fixes varied as follows depending on the type of method used: Cell site: 800 to 2000 meters; A-GPS: 10 to 20 meters; GPS: 10 to 80 meters; Cell site + WiFi: 60 to 250 meters.

carrier's firewall and then further aggregating the data before packaging the data for sharing with third parties.

Third, heightened security safeguards can also help ensure that location data is not misused by unauthorized individuals. Hashing of location data, use of encryption, restricting access to keys as well as other physical, administrative and technical safeguards typically used to protect sensitive data can be implemented.

Fourth, use of appropriate anonymization and aggregation techniques can also help ensure that potentially linkable location data will not be misused. CTIA – the Wireless Industry Association has developed guidelines effectively and widely-adopted by the mobile industry to promote and protect user privacy in the area of Location-Based Services ("LBS").[7] These guidelines support the broadly accepted principle that notice is adequate where anonymization and aggregation techniques remove or permanently obscure information that identifies a specific device or user.[8] We acknowledge that there are still some challenges in the area of anonymization highlighted by the AOL and NetFlix incidents.[9] We address the need to encourage development of industry standards around appropriate anonymization and aggregation techniques further below.

AirSage notes that this is not an exclusive or exhaustive list and any safe harbor should be technologically neutral and not overly prescriptive.

C. Impact to Market, Consumers and Public Services Reliant on Location Data is Significant if Rules Around Location Data Use are Overly Broad.

Should collection or use of location data be curtailed, the impact to the mobile marketplace, mobile consumers and public services that rely on location data would be significant. According to surveys, two-thirds of wireless service providers expect advertising to generate up to 10 percent of their revenue in the next five years. Almost a third project advertising to contribute to over 10 percent of their revenue. Without these revenue streams, wireless service providers and application developers will have less incentive to continue to develop and create free mobile applications.

With a decrease in availability of free mobile applications, consumers would either have to forgo such products and services or take on the burden of the costs associated with the benefit of use and enjoyment of these applications. Consumers would also receive less of the benefits of location-enhanced mobile services generally. Moreover, mobile consumers who

---

[7] CTIA's "Best Practices and Guidelines for Location Based Services" are available at http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf.

[8] *Id*. at 2.

[9] In 2006, AOL released a list of 20 million web search queries that were purportedly anonymized because users were identified with only a number. The New York Times nevertheless tracked down one of the users through only their search terms. *See* Michael Barbaro & Tom Zeller Jr. *A Face is Exposed for AOL Searcher No. 4417749*, NY Times, August 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html. Similarly, Netflix released "anonymous" movie ratings of 500,000 subscribers in the course of a contest challenging researchers to improve its recommendation engine, and some of the records were de-identified by comparing the records to public ratings at the Internet Movie Database. *See* Arvind Narayanan and Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

expect and demand a faster, easier experience when using mobile applications will find the alternative of numerous pop-ups and interruptions to be a frustrating experience that is, for many consumers, not outweighed by their concerns where the data is already processed, anonymized and aggregated in a manner that safeguards their privacy.

The public sector will also be impacted greatly. The location data relied on by traffic planning and disaster response managers is largely sourced from the same pool of data used for marketing and providing location services to consumers. A reduction of the quantity and quality of that pool of data would greatly impact infrastructure planning agencies that would not otherwise be able to replicate that data without a very high cost.

IV. Anonymized Data

Commission staff also seeks input on what technical measures exist to more effectively "anonymize" data, and whether industry norms are emerging in this area. AirSage recognizes that industry standards are still developing but believes that effective anonymization techniques are being implemented by many analytics service providers as a means to help prevent inadvertent linking of data.

A safe harbor for demonstrated proper use and handling of linkable data should include a commitment to implementing effective anonymization techniques. Development of a standard should be based on those accepted and used today by responsible analytics service providers like AirSage.

Anonymization techniques used by AirSage and others include a) removing not only personally identifiable information but also non-obvious identifiers that combined with other data, could easily allow an outside party to infer individual identity, b) use of unique numbers or codes (pseudonymization) in place of identifying information, c) ensuring pseudonymization or removing or masking of identifiers are not easily reversible, d) when using a hash algorithm to create pseudonyms, ensuring the hash is randomized and not reversible, e) appropriate safeguarding of the algorithm method and use of firewalls and other data segregation techniques to prevent disclosure of raw individual level data used to create anonymized or aggregated data, and f) rules for minimum levels of aggregation to avoid reports that inadvertently increase risk of identification.

We note that the anonymization techniques we suggest should not be prescriptive, nor is a checklist approach to all these factors appropriate or necessary. Instead, any anonymization standard or policy should be scalable and the degree to which various techniques are applied should be based on an initial assessment of the potential privacy risks associated with the data set in question.

V. Conclusion

AirSage thanks the Commission for its attention to the important privacy issues that relate to linkable data and location data. We appreciate the opportunity to submit these comments and hope that our input will assist Staff with an understanding of the industry complexities and importance of location data to industry, consumers and the public and our recognition and willingness to contribute to development of anonymization and aggregation

standards based on our wide and deep experience. As the FTC continues to clarify the scope and application of the framework, AirSage welcomes further opportunity to continue a dialogue to contribute to understanding around these important privacy issues as applied to the unique challenges and benefits of the mobile industry.

Cy Smith
Founder and President AirSage, Inc.
400 Embassy Row NE Suite 100
Atlanta, Georgia 30328