UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Division of Privacy and Identity Protection

September 10, 2012

By First Class Mail

Carolyn J. Merry, PhD
COGO Chair
Professor and Chair
Department of Civil, Environmental and Geodetic Engineering
The Ohio State University
470 Hitchcock Hall
2070 Neil Avenue
Columbus, Ohio 43210-1275

Re: *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*

Dear Professor Merry:

Thank you for your June 29, 2012 letter on behalf of the Coalition of Geospatial Organizations to Federal Trade Commission ("FTC" or the "Commission") Chairman Jon Leibowitz, regarding the Commission's March 2012 report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("Privacy Report").[1]

In your letter, you express concern about the use of the term "precise geolocation data" and the obligations that the Privacy Report imposes upon geospatial industry members' professional activities. More specifically, you state that footnote 187 "does not protect the provider of the data in the case of physical addresses, parcel information, or other geolocation or survey data tied specifically to public land records, because the information can ultimately be linked back to the owner or occupant of record."

By way of background, the FTC's Privacy Report builds on a series of public roundtables that brought together various stakeholders to discuss the privacy issues and challenges associated with current and developing technology and business practices that collect and use consumer data. Following these roundtables, FTC staff issued a preliminary report that discussed the themes and areas of consensus developed through the roundtables and called for public comment on a series of questions related to a proposed privacy framework. Based upon the more than 450 comments received – including many from members of the geospatial industry – in March of this year, the Commission issued its Privacy Report and set forth a final privacy framework for companies that collect and use

[1] Privacy Report, *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

consumer data for commercial purposes. The final privacy framework calls on companies to incorporate the following practices into their business operations: (i) privacy by design – build privacy into products and services through every stage of development; (ii) simplified consumer choice – give consumers the ability to make decisions about their data at a relevant time and context; and (iii) increased transparency – make data collection and use practices more transparent.[2]

In developing the simplified consumer choice concept, the Commission sought to reduce the burden on consumers who wish to seek greater control over the collection and use of their personal information. At the same time, the Commission recognized that there are a variety of important benefits that come from the collection and use of consumer data. In order to balance these two interests, the framework calls on companies to offer an effective consumer choice mechanism unless the data practice is consistent with the "context of the interaction" between the consumer and the company. Under this standard, whether a company should provide choice "turns on the extent to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law."[3]

Rather than enumerating a fixed list of specific data practices that merit consumer choice and those that do not, the Commission's context of the interaction standard is designed to be sufficiently flexible to allow businesses to innovate and develop new products, services, and business models. In order to provide illustrative guidance in applying the standard, the Privacy Report discusses examples of practices – such as fraud prevention and certain types of first-party marketing – that are likely to be consistent with the context of the interaction and therefore would not need consumer choice.

In response to your question about whether members of the geospatial industry that collect addresses, parcel information, or other geolocation or survey data that is tied to public land records must offer a consumer choice mechanism, staff believes that this practice would generally fall within the context of the interaction standard. Indeed, as any consumer who has purchased a house knows, public land record data is collected, used, and linked to specific consumers as a matter of course in connection with real estate transactions as well as property tax assessments and similar purposes. Accordingly, we believe the collection and use of this data for these purposes would not trigger an obligation to provide a consumer choice mechanism.

It is noteworthy that, given its public nature and availability, geolocation data that is tied to public land record information differs markedly from other types of geolocation data. For example, precise geolocation data – such as information collected through a consumer's use of a Global Positioning System application on a smart phone – that reveals a consumer's movements in real time and over time is particularly sensitive and raises heightened privacy concerns.[4]

---

[2] The framework also incorporates the well-established Fair Information Practice Principles and is consistent with the Department of Commerce's parallel privacy initiative. *See* Privacy Report, at i, 3.

[3] *Id.* at 38-39.

[4] *Id.* at 33, 58-60.

Finally, it should also be noted that the Commission's privacy framework is a voluntary set of best practices designed to help "companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses."[5] The framework thus does not impose any new legal obligations on the geospatial or any other industry. As specially stated in the Privacy Report, the framework "is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC."

Sincerely,

Maneesha Mithal /CNO

Maneesha Mithal
Associate Director
Division of Privacy and Identity Protection

[5] *Id.* at 1.