Interactive Advertising Bureau
116 E. 27th St. 7th Floor
New York, New York 10016
212.380.4700

June 4, 2014

The Honorable Al Franken
Chairman, Senate Judiciary Subcommittee on Privacy, Technology and Law
223 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Jeff Flake
Ranking Member, Senate Judiciary Subcommittee on Privacy, Technology and Law
153 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Franken and Ranking Member Flake –

I am writing to express the IAB's concerns with S. 2171, the Location Privacy Protection Act. The Interactive Advertising Bureau (IAB) is the leading trade association for the more than 600 media and technology companies that serve and sell digital advertising. While only a small share of the overall $43 billion industry today, mobile advertising in the United States is rapidly growing and totaled $7.1 billion during FY 2013, a 110% increase from the prior year total of $3.4 billion. A share of that growth is attributable to the explosion of location based services unique to consumers' mobile behavior.

The IAB takes consumer privacy very seriously. IAB serves as the Chair of the Board of Directors at the Digital Advertising Alliance (DAA) – the independent, regulatory arm of the industry. The DAA began offering real notice and choice to consumers about data collected for advertising in 2010, expanded the program to include all data collection and strict prohibitions on specifics uses in 2011, and again expanded the program to include mobile applications, and consent to collect precise geo-location data and personal directory data in 2013. The DAA has been recognized by the White House, the Federal Trade Commission, and the Department of Commerce as an example of successful self-regulation. IAB's commitment to the program extends to our member companies, who must publicly adhere to the program as a condition of membership.

IAB is concerned with the bill's conflation of legitimate commercial uses of data that deliver concrete benefit to consumers, with that of abusive criminal behavior. The misappropriation of a user's data for criminal activity is distinctly different from the legitimate commercial practices that consumers have come to expect and value; and, is responsible for much of the free or low-cost digital services and applications we enjoy today.

For example, the definition of geolocation information is very broad; and, would sweep in location data that cannot identify an individual or device with specificity. This broad definition is appropriate to address criminal uses where a broad-based location data point still presents great harm to an identifiable victim; while, anonymous, general location data for marketing purposes such as couponing or promotion of local small business is not identifiable and does not pose the same risks as criminal abuses. Furthermore, the definition does not exempt data collection requested by the user, and necessary to provide a service such as a mapping application or GPS device, which is likely to result in added confusion.

The breadth of data covered by this definition is further compounded by the consent requirements. Prohibition on collection or disclosure of geolocation information without express informed consent is tied to the "individual using the device" rather than the owner of the device or the settings on the device. This significantly hinders the use of devices with multiple users, such as tablets, requiring separate consent from each user each time the device changes hands.

Friction is the greatest enemy to the consumer experience, and a company's success in the marketplace. When multiple permission and disclosure screens stand between the consumer and the content they seek, the consumer does not become more educated about data collection practices, they become frustrated.

Innovation and consumer privacy are not competing interests. In fact, consumer privacy is one of the leading areas of innovation evidenced by the proliferation of services like Whisper, Snapchat, Line, and Tango; and, by leading platforms like iOS and Android competing on granular privacy controls for consumers.

In the rapidly evolving mobile technological environment, industry is continuously adapting to new technologies and innovation in the marketplace to meet consumer needs and preferences. Current industry practice is to acquire consent to collect location data from mobile devices. S. 2171, however, would codify current practice, creating a disincentive for companies to develop new or innovative means for transparency and consumer control over data collection practices. Self-regulation allows industry to pivot as the marketplace changes – the DAA has updated its code of conduct twice in less than two years.

The most recent update to the self-regulatory program, the application of self-regulatory principles to the mobile environment, was released in July 2013 and implementation begins this year. We respectfully ask the Committee to consider the complicated legal regime created by applying criminal standards to commercial regulation; and, to allow the DAA the opportunity to build on its great success by implementing and enforcing the application of self-regulatory principles to the mobile environment.

Respectfully,

/s

Mike Zaneis
EVP & General Counsel
Interactive Advertising Bureau