

Senator Warren Introduces Bill to Ban the Sale of Location and Health Data

New Media and Technology Law Blog on June 16, 2022

On June 15, 2022, Senator Elizabeth Warren [introduced](#) a bill, cosponsored by a host of other Democratic and independent Senators, the “[Health and Location Data Protection Act of 2022](#),” which, subject to a few exceptions, would, among other things, prohibit the selling, sharing or transferring location data and health data. The bill gives the Federal Trade Commission (FTC) rulemaking and enforcement authority for violations of the law and also grants state attorneys general the right to bring actions; notably, the law would also give a private right of action to persons adversely affected by a violation of the proposed law.

Some major provisions of the bill:

- **Definition of “Data” and “Location Data”:** “Data” includes “information that is linked, or reasonably linked to specific individuals, or specific groups of individuals who share the same place of residence or internet protocol address.” The term “location data” is defined as “data capable of determining the past or present physical location of an individual or an individual’s device” (note: the bill does not make a distinction between geolocation data and *precise* geolocation data). It would be interesting to see how the term “reasonably linked” in the definition of “data” would be interpreted, as location data is often anonymized before it is packaged and sold (yet, in some instances, may theoretically still be able to be de-anonymized). To the extent a mobile app that collects locational data aggregates it before transferring it to a third party, it may be outside the scope of the act.
- **Definition of “Data Broker”:** The bill defines a data broker as a person that collects, buys, licenses, or infers data about individuals and then sells, licenses, or trades that data. Thus, an app publisher that collects Location Data would be considered to be a Data Broker under this bill. This is a more expansive view of what a data broker is as compared to the current state laws addressing data brokers. See e.g., [Civ. Code § 1798.99. 80\(d\)](#) (California’s data broker registration law defines “data broker” as: “a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship”).

- **Prohibition and Exceptions:** The bill would make it unlawful for a data broker to “sell, resell, license, trade, transfer, share, or otherwise provide or make available” location data or health data (or categories of such data as the FTC may identify). The bill makes exceptions for health information transfers done lawfully under HIPAA, publication of “newsworthy information of legitimate public concern” under the First Amendment, or disclosure for which the individual provides “valid authorization.” The FTC would be responsible for adapting the HIPAA-related term “valid authorization” to fit the location data context. It is possible that the conspicuous notice and consent processes surrounding the collection and use of the data – as is currently in place in many mobile applications – will suffice.
- **Enforcement:** The bill empowers the FTC, state attorneys general, and injured persons to sue to enforce the provisions of the law. With regard to the FTC, the text states that a violation of the law would be deemed an unfair or deceptive practice under the FTC Act, and specifically allows the FTC to pursue injunctive relief, deletion of data and obtain civil penalties (as defined under the bill). The private right of action in the bill would give “any person whose interest has been or is threatened or adversely affected by the engagement of any data broker” to seek injunctive relief, deletion of data, monetary damages and attorney’s fees.

Public awareness and general scrutiny over the collection, selling and packaging of geolocation data has heightened in recent years, earning the attention of both federal and state regulators and legislatures. This is not the first bill introduced in Congress in recent years that has attempted to generally limit the sale of mobile location data. (There are even provisions covering “sensitive covered data” (which include location data) in the recently released [discussion draft](#) of the bipartisan federal data privacy bill that would prohibit the transfer of an individual’s precise geolocation data to a third party, absent affirmative express consent). Notably, this bill comes on the heels of two [letters](#) sent by Senator Warren and others to data analytics companies inquiring about their locational data tracking with respect to visits to Planned Parenthood centers.

[View Original](#)

[Related Professionals](#)

- **Jeffrey D. Neuburger**