MEMORANDUM

TO: New Jersey General Assembly

DATE: March 24, 2021

FROM: Lisa McCabe, Director, State Legislative Affairs

RE: Opposition to Assembly Nos. 2340 and 2489

On behalf of CTIA, the trade association for the wireless communications industry, I write in opposition to Assembly Nos. 2340 and 2489, which prohibit a commercial mobile service provider from disclosing a customer's geolocation data to a third party, unless the customer has given consent. This legislation is unnecessary, would add to the further fragmentation of consumer privacy laws, and raises particular concern because it is technology-and-sector-specific.

Consumer privacy protections should apply consistently across all industry sectors, and protections should be consistent for any given type of information. These bills applies to a specific type of information – geolocation information – that is collected from a mobile device. Because the requirements in the bill only apply to geolocation data, the legislation favors certain business models and particular competitors over others. For instance, many online companies have access to location data on consumer handsets and use that data for a variety of purposes. Operating system platforms can collect large amounts of location data from WiFi access points and sell ads based on this data. WiFi networks provide greater location accuracy and various third parties have mapped these networks. Nevertheless, the proposed law would not apply in these situations in which precise location data is collected, used, and shared. This legislation is unfairly limited to the collection of one type of location data in the online ecosystem – something that consumers are unlikely to understand or expect.

Passage of A2340 and A2489 could cast doubt on the legitimacy of ordinary business operations, which may require consent for the disclosure of information to service providers. For example, if a provider sees a consumer logging into an online account from New Jersey, but the consumer's cell phone is located in Montana, that alerts the provider to possible fraud. If a customer's login occurs from a New Jersey IP address, and the same customer's cell phone location recently registered in New Jersey, that is a sign the consumer is traveling. The broad definition of disclosure and the lack of a clear exception for service providers in the bill make it unclear as to whether fraudsters must opt in for commercial mobile service providers to use such information to protect consumers. Additionally, these bills create ambiguities for how some ordinary apps function. For example, would consent be required if location had to be transferred to another carrier or service provider in order to make the app function? If a consumer uploads a photo or data containing geolocation information from her phone to an app or cloud storage service, does this constitute disclosure? What if the consumer requests such a transaction but does not provide the consent necessary to complete the transaction?

Privacy issues are better addressed with a holistic approach that does not apply differently to different types of data or favor one business model over another, in order to lessen any unintended consequences and provide consistent consumer protections. For these reasons, CTIA respectfully requests that you oppose Assembly Nos. 2340 and 2489.