White Paper
Geolocation Data Mandates Legislation
New Jersey A2340/S1832

Introduction

CTIA®, the trade association for the wireless communications industry, submits this white paper outlining concerns regarding New Jersey A2340/S1832, which prohibits commercial mobile service providers from disclosing customer's global positioning system data to third parties, unless the customer has given consent. This legislation raises particular concern because it is technology-and-sector-specific, could impede important services, such as prevention of consumer fraud, would add to the further fragmentation of consumer privacy laws, and is unnecessary.

Consumer privacy protections should apply consistently

Consumer privacy protections should apply consistently across all industry sectors, and protections should be consistent for any given type of information. Because the requirements in the bill only apply to geolocation data used by mobile service providers, 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. Other entities can collect large amounts of location data in other ways and sell ads based on this data. The proposed law would not apply in all 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.

This legislation could increase consumer frustration and reduce consumer fraud protection

This legislation would add to consumer frustration and notice fatigue in which consumers stop paying attention – but businesses would still be faced with the burden of presenting and recording these consents.

Additionally, location information plays an important role in fraud prevention, which could be impeded by this type of legislation. Many businesses use location information to identify and combat fraud on behalf of customers. Without the use of this information, bad actors could more easily use a consumer's identity fraudulently. Location technology can be used to automatically block suspect traffic, request verification (via email or SMS), or flag suspect

activity for further internal review. It can also be a key marker to identify at-risk devices used by would-be identity thieves.

This legislation would make it difficult for businesses operating in New Jersey to provide important services to consumers

Passage of A2340/S1832 could cast doubt on the legitimacy of ordinary business operations. 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?

Additionally, while the legislation makes important exceptions for information provided to emergency service organizations, among others, it does not make an explicit exception for information shared with a carrier's service providers or vendors, which can create operational challenges.

Federal & state laws already exist providing consumer protections

Wireless service providers have committed to obtain affirmative opt-in consent of their wireless consumers before using or sharing subscribers' precise location information – with limited exceptions for emergency situations and appropriate legal process[1]. This is consistent with the Federal Trade Commission's (FTC) Privacy Framework, which considers precise geolocation information to be sensitive, meaning that its collection must be subject to opt-in consent. The FTC regularly brings enforcement actions against companies that have misrepresented consumer control regarding collection and use of geolocation data.[2]

[1] https://api.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf

[2] See, e.g., *In the Matter of InMobi Pte Ltd., a private limited company.* F.T.C. June 22, 2016. 3:16-cv-03474; *In the Matter of Nomi Technologies, Inc., a corporation*. F.T.C. September 3, 2015. 132-3251; *In the Matter of Goldenshores Technologies, LLC, a limited liability company, and Erik M. Geidl, individually and as the managing member of the limited liability company.* F.T.C. March 31, 2014. 132-3087.

In particular, in the mobile world, there are federal protections for consumers that govern wireless carriers' use of the location data they have as a means to provide their customers service. The Federal Communications Commission (FCC) has jurisdiction over wireless telecommunications providers. Federal law and regulations generally require telecommunications carriers to obtain opt-in consent prior to sharing mobile call location information.

In addition, the New Jersey Attorney General already has the authority to address unfair or deceptive acts or practices relating to consumer privacy under state consumer protection laws.

A private right of action would harm businesses with no benefit for consumers

Enforcement agencies such as the state attorneys general should shape statewide policy with a more holistic and experienced approach. Agencies can be expected to better understand the complexities of the law and to balance the various factors of encouraging compliance, supporting innovation, and preventing and remediating harm. The Attorney General can also ensure consistent interpretation and application of the law, which benefits businesses and consumers alike.

The private right of action allowed for in this bill will unfairly expose wireless service providers operating in New Jersey to costly litigation and will not benefit consumers.

According to a study prepared by Hogan Lovells for the U.S. Chamber Institute for Legal Reform, plaintiffs rarely recover from lawsuits brought in privacy-related cases. Instead, this litigation "often leads to a major payday for plaintiffs' attorneys, even where class members experienced no concrete harm . . . even where class members may have suffered a concrete injury, the data indicates that they are unlikely to receive material compensatory or injunctive relief through private litigation."[3] Recent data on the California Consumer Privacy Act (CCPA) suggests that the inclusion of any private right of action in a bill, however limited, appears to invite litigation. Although the CCPA strictly limits private litigation to data security breaches, over half of the cases brought in its first year raised broader claims that the law appears to foreclose.[4] In 2020 alone, 75 class action suits were filed citing the CCPA.[5] The inclusion of a

[3] Mark Brennan et al., *Ill-Suited: Private Rights of Action and Privacy Claims*, U.S. Chamber Institute for Legal Reform (July 2019).
[4] Perkins Coie, *CCPA Litigation Year in Review* (March 21, 2021), available at CCPA Litigation Year in Review | Perkins Coie.
[5] Akin Gump, 2020 CCPA Litigation Report (March 23, 2021), available at Akin Gump Announces 2020 CCPA Litigation Report.

private right of action will significantly increase the cost of offering mobile applications in New Jersey.

In short, allowing for a private right of action in privacy legislation like this would subject companies, both large and small, to the risk of expensive litigation that primarily benefits the plaintiff's bar and offers little relief to consumers.

Activity on privacy is taking place in Congress

Momentum for baseline privacy legislation that offers consistent protections for all U.S. consumers has been building, and the 117th Congress is widely seen as likely to pass such legislation.[6] There is bipartisan interest in this issue in Congress, where numerous hearings have been held and many of the concepts in bills pending in the Senate and the House have widespread support. The FTC has also announced its interest in undertaking rulemaking on privacy in the coming months if sufficient momentum does not occur in Congress.[7] A uniform law that covers all types of personal data and the different companies that collect it is the best approach for U.S. consumers and businesses.

The marketplace is addressing consumer privacy concerns

The marketplace is developing solutions to address consumer privacy concerns.[8] Apple recently released a privacy feature, App Tracking Transparency, in its iOS 14.5 version that requires any app that wants to track a user's activity and share it with other apps or websites to ask for permission.[9] Apps that do not comply will be blocked from download on Apple devices. Similarly, Google plans to phase out third-party cookies from its Chrome browser by 2022, and it does not plan to build alternate identifiers to track individuals as they browse across the web, nor will it use them in its products.[10]

---

[6] Jennifer Bryant, *2021 'best chance' for U.S. privacy legislation*, International Association of Privacy Professionals (December 7, 2020), available at 2021 'best chance' for US privacy legislation (iapp.org); Rebecca Klar and Chris Mills Rodrigo, *New state privacy initiatives turn up heat on Congress*, The Hill (February 10, 2021), available at New state privacy initiatives turn up heat on Congress | TheHill.

[7] Megan Brown and Duane Pozza, *FTC prepares to expand rulemaking, including on privacy and data use*, JD Supra (March 31, 2021), available at FTC Prepares to Expand Rulemaking, Including on Privacy and Data Use | Wiley Rein LLP - JDSupra; Pres Release: FTC Acting Chairwoman Slaughter Announces New Rulemaking Group (March 21, 2021), available at FTC Acting Chairwoman Slaughter Announces New Rulemaking Group | Federal Trade Commission.

[8] https://www.washingtonpost.com/business/apple-and-google-are-killing-the-adcookie-heres-why/2021/04/26/9e9bbd50-a67e-11eb-a8a7-5f45ddcdf364_story.html

[9] https://www.wsj.com/articles/ios-14-5-a-guide-to-apples-new-app-tracking-controls-11619457425

[10] https://blog.google/products/ads-commerce/a-more-privacy-first-web/; https://www.washingtonpost.com/business/apple-and-google-are-killing-the-adcookie-heres-why/2021/04/26/9e9bbd50-a67e-11eb-a8a7-5f45ddcdf364_story.htm

Conclusion

Because of the reasons detailed above, no other state has passed legislation specifically regulating location information through a standalone bill. Location information itself and the ways it is used to deliver service to consumers are often difficult to define and to regulate without unintended consequences. It is challenging to draft a bill that is both operationally workable and improves consumer protection—two goals that this bill falls short on.

Privacy issues are better addressed with a holistic approach and at the federal level so that the law does not apply differently to different types of data or on a patchwork, state-by-state basis, or favor one business model over another. A consistent and comprehensive approach will lessen any unintended consequences and best protect consumers.