BCLP. Client Intelligent

Insights

PRECISE GEOLOCATION: RECENT TRENDS AND ENFORCEMENT

Mar 29, 2023

"Precise Geolocation" has become a hot button issue in the privacy world with recent data privacy laws seeking to regulate the collection and processing of such information, including in California and Virginia.[1] The definition of "Precise Geolocation Data" varies by state but generally means "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of" a certain distance.[2] The majority of state-level privacy laws now categorize Precise Geolocation Data as "sensitive personal information."[3] This classification gives rise to additional obligations for organizations that collect and process Precise Geolocation Data. For example:

- California Law: In-scope organizations that collect and process "sensitive personal information," including Precise Geolocation Data, must provide Californians with the right to limit that organization's use of "sensitive personal information," subject to certain exceptions.[4]
- Virginia Law: In-scope organizations must obtain consent to process "sensitive data," including Precise Geolocation Data, as well as conduct and document data protection assessments.[5]

UPDATES TO THE NAI FRAMEWORK

Certain self-regulatory bodies, like the National Advertising Initiative ("**NAI**"), are also updating their guidance relating to the collection of Precise Geolocation Data.[6] The NAI, an industry trade group that develops self-regulatory standards for online advertising, recently released a set of voluntary standards to be used by Location Solution Providers ("Providers")[7] that collect and use Precise Geolocation Data in the products they offer.[8] According to the NAI, the goal of these standards is to reduce the collection of information specific to a particular point of interest (*e.g.* a storefront location) that an average person may consider sensitive or detrimental to their privacy. The NAI recommended that its members avoid collecting data concerning certain sensitive points of interest such as places of worship, places that imply LGBTQ+ identification, welfare or homeless shelters, and halfway houses.[9] The NAI also states that Precise Geolocation Data should not be used, sold,

or shared for law enforcement, national security, or bounty-hunting purposes, except as necessary to comply with an organization's valid legal obligations.[10] Any Provider that collects Precise Geolocation Data and chooses to publicly commit to the NAI standards may be assessed for compliance, and violations of the standards may result in enforcement and sanctions by the NAI, as well as potential enforcement actions by the Federal Trade Commission ("FTC").[11]

THE FTC WEIGHS IN

The federal government and its regulatory agencies also are focusing on organizations that use Precise Geolocation Data, as evidenced by a July 2022 publication[12] and recent enforcement actions, including a recent suit against an Idaho-based data broker[13], alleging that it sold Precise Geolocation Data associated with hundreds of millions of mobile devices.[14] The FTC argued that this information could be used to trace the movements of individuals to and from certain locations, including reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities.[15] The FTC argued the selling of this information could enable others to identify individuals and expose them to threats of stigma, stalking, discrimination, job loss, and even physical violence.[16] The FTC sought to halt the sale of the Precise Geolocation Data and have the information deleted.[17] As of this writing, the matter is pending.

NEXT STEPS AND OTHER CONSIDERATIONS

The shift towards scrutiny of Precise Geolocation Data should put organizations on notice that longstanding data practices utilizing Precise Geolocation Data may have to be reassessed. Organizations using Precise Geolocation Data should be aware that regulators at the state and federal level are now aggressively policing this area and this trend is likely to continue. Certain organizations, like Apple, have also reacted to this issue by enforcing development rules related to collection of Precise Geolocation Data.[18] Apple, through its Location Services function, provides individuals with control over Precise Geolocation Data collection and processing activities for apps that are available on the App Store.[19] An individual must enable Location Services, before Precise Geolocation Data can be collected and used.[20] Similarly, Google and applications available through the Google Play store may ask permission and obtain consent from individuals in order to collect and use Precise Geolocation Data.[21]

As such, organizations collecting and using Precise Geolocation Data should:

1. Understand whether and what type of geolocation data is being collected (Precise Geolocation Data vs. general location data);

2. Understand the legal differences between the types of geolocation data (Precise Geolocation Data vs. general location data) being collected;

3. Map existing and future uses of Precise Geolocation Data to better understand when and in what solutions and services they collect and use Precise Geolocation Data;

4. Ensure privacy notices accurately describe Precise Geolocation Data collection and usage, particularly for mobile applications;

5. Confirm that the NAI standards are being followed if you are a Provider that collects Precise Geolocation Data and has publically committed to following the NAI standards;

6. Develop a clear and actionable strategy for obtaining consent[22] for the collection and use of Precise Geolocation to the extent required under applicable state privacy laws; and

7. Review the collection and use of Precise Geolocation Data in California to determine whether any use is subject to California's right to limit, as described above.

If you have any questions relating to these complicated issues, please reach out to a member of our Data Privacy and Security team at Bryan Cave Leighton Paisner LLP.

---

[1] California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"), Cal. Civ Code §§ 1798.140 (ae) and 1798.121 (does not require opt-in consent, but instead the collection and processing of Precise Geolocation Data is subject to an opt-out in certain circumstances); Virginia Consumer Data Protection Law ("VCDPA"), Va. Code § 59.1-517 (requires opt-in consent for the collection and processing of Precise Geolocation Data). Other state ombinbus privacy laws, such as the Connecticut CTDPA (requires opt-in consent for the collection and processing of Precise Geolocation Data) and Utah UCPA (does not require consent for the collection and processing of Precise Geolocation Data but the processing of such information cannot occur without first presenting the consumer with a clear notice and an opportunity to opt-out of the processing) also regulate Precise Geolocation Data. Connecticut Substitute Bill No. 6 § 1(27); Utah Civ. Code § 13-61-101(32(a). The Colorado Privacy Act ("CPA") does not include Precise Geolocation Data in its definition of "sensitive data," but generally does require consent for the collection and processing of "sensitive data." Col. Rev. Stat. § 6-1-1301.

[2] *Id.* Under the CPRA, the degree of accuracy and precision for Geolocation Data is a radius of 1,850 feet or less. Whereas, under other state privacy laws, the radius is 1,750 feet or less.

[3] *Id.*

[4] Cal Civ. Code § 1798.121. Under California law, specifically the CCPA/CPRA, organizations that collect and process "sensitive personal information" must provide Californians the right to limit the use of that "sensitive personal information" but only in certain circumstances. These organizations must give notice to consumers and must include "a clear and conspicuous" link on the company's website that will let the consumer limit the use and disclosure of personal information. When a

request is received, the organization will have to limit its processing of this information to certain enumerated "business purposes" under the CCPA/CPRA and require its vendors or service providers to do the same.

[5] Va. Code § 59.1-517. Organizations must collect consent from an individual if “sensitive personal information” is being processed. Further, these organizations must undertake and document what is called a “data protection assessment” for the collection and use of this information.

[6] The National Advertising Initiative, available at https://thenai.org/.

[7] NAI Precise Location Information Solution Provider Voluntary Enhanced Standards, available at https://thenai.org/accountability/precise-location-information-solution-provider-voluntary-enhanced-standards/. Location Solution Providers are NAI member companies that collect Precise Geolocation Data and use it to provide location-based audiences or other analytical services to clients.

[8] *Id.*

[9] *Id.* at page 2. The NAI also lists other sensitive points of interest not to be collected: correctional facilities; places that may be used to infer engagement with explicit sexual content, material, or acts; places primarily intended to be occupied by children under 16; domestic abuse shelters, including rape crisis centers, dependency, or addiction treatment centers; medical facilities that cater predominantly to sensitive conditions, such as cancer centers, HIV/AIDS, fertility or abortion clinics, mental health treatment centers, or emergency room trauma centers; places that may be used to infer refugee or immigrant status, such as refugee or immigration centers and immigration services; credit repair, debt services, bankruptcy services or payday lending institutions; temporary places of assembly such as political rallies, marches, or protects, during the times that such rallies, marches, or protests take place; military bases.

[10] *Id.* at page 3.

[11] *Id.* at page 1.

[12] Federal Trade Commission, Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data, https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal (highlighting the agency’s continued focus on “highly sensitive data,” including information about a person’s health and precise location data).

[13] Federal Trade Commission v. Kochava, Inc., Case No. 2:22-cv-377, complaint at https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf; see also Federal Trade Commission, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations, available at https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] Apple, Location Services & Privacy, available at https://www.apple.com/legal/privacy/data/en/location-services/.

[19] *Id.*

[20] *Id.*

[21] Android Developers, Request Location Permissions, available at https://developer.android.com/training/location/permissions; Google, Choose Which Apps Use Your Android Phone's Location, available at https://support.google.com/accounts/answer/6179507?hl=en.

[22] In jurisdictions requiring that consent be captured prior to the collection and processing of Precise Geolocation Data, that consent must be affirmative and informed. This requires a notice that details and allows for the collection of Precise Geolocation Data, and clearly explains the method through which this data will be collected, as well as the purposes for which the data will be used. Affirmative consent requires the individual to take a clear and specific action. This could include having to click through a splash page or pop-up box before continuing to an application or website. The consent should be recorded and documented by the business and there likely will need to be a mechanism to withdraw the consent.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448