FUTURE OF PRIVACY FORUM

Policy Brief: Location Data Under Existing Privacy Laws

December 2020

Stacey Gray, FPF Senior Counsel

Pollyanna Sanderson, FPF Policy Counsel

Defining and regulating location data in a privacy law can be an elusive challenge. In part, this is due to its ubiquity in our lives: information about how devices and people move through spaces over time is utilized by Wi-Fi networks, smartphones, mobile apps, and a world of emerging screenless technologies, such as wearable fitness devices, scooters, autonomous vehicles, and video analytics. Existing legal and self regulatory regimes in the United States (and globally) approach location data in a variety of ways that may serve as a model for policymakers.

Challenges of Defining Location Data

Location data can be challenging to define and regulate. This is in part because even the most basic device connectivity typically involves a variety of information that allows content providers, apps, platforms, OS providers, and others to learn the general or specific location of that device. For example, a device's IP address, which is necessary to send and receive Internet content, is often sufficient to learn a user's approximate location (city or state). Location data can also be determined from a wide variety of technologies embedded in modern devices, such as GPS chips, Bluetooth, or proximity to local cell towers and networks.

In addition, smartphone apps typically receive approximate or precise location information through user permissions, in order to provide navigation, ride-sharing, games, or weather alerts. Apps often use, share, or sell location data for additional purposes, such as advertising, fraud detection, or location intelligence and analytics. Increasingly, "screenless" technologies also use location data, such as scooters, e-bicycles, and autonomous vehicles, raising challenges for notice and consent.

When is Location Data "Personal"?

Location data is considered "personal information" under most, if not all, privacy laws around the world, when the data **relates to an identifiable person.** For example, precise location data involving buildings, landmarks, or factory sensors are usually not personal information. Similarly, aggregated data (information about movements of large groups) is not considered personal information.

Location data is personal information when it is sufficiently **precise, accurate,** and/or **persistent** (collected over time) to identify a person with reasonable specificity.

Precision refers to the granularity of a location measurement. For example, a specific street corner is more precise than a city or country. In a rural or remote area, a lower level of specificity might be more able to identify a person than if that same person were standing in Times Square. For this reason, numeric cut-offs (such as a 1,640 foot radius) may provide clear bright lines, but can sometimes be over or under-inclusive.

Accuracy refers to whether or not the data reveals the true location of a device. The more accurate the data, the more revealing it tends to be, and the greater the risks of re-identification.

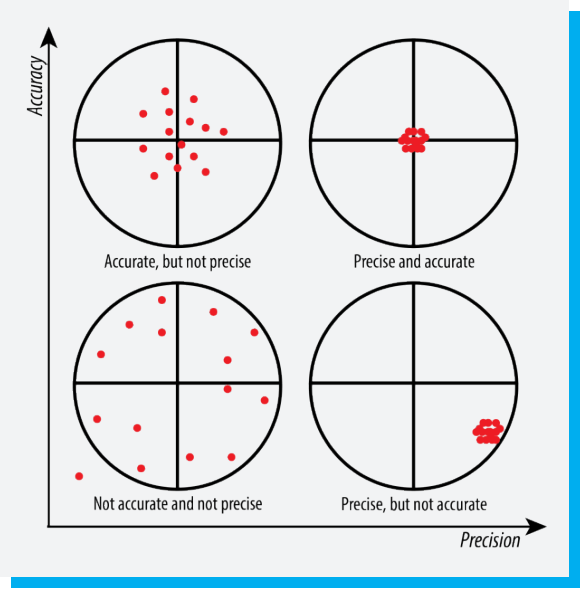

Figure 1. Precision vs. Accuracy. Source: St. Olaf College, https://wp.stolaf.edu/it/gis-precision-accuracy/.

Persistence refers to the frequency of the collection of location data, as well as the length of time over which it is collected. Short term, transient location information is typically less identifiable or revealing than long-term, persistent location history.

Legal Protections in the U.S. and Globally

In the United States, legal protections for location data exist in the U.S. Constitution,

the Federal Trade Commission's (FTC) Section 5 of the FTC Act, and a variety of federal and state laws. The Network Advertising Initiative (NAI) also provides self-regulation for location data in its Code of Conduct. Globally, protections for location data also exist in many legal regimes, including the GDPR and PIPEDA.

Legal protections vary. For example, in the law enforcement context, precise location data requires a warrant in the United States. In commercial settings, location data usually requires affirmative opt-in consent, such as when collected from mobile apps (under the FTC Act) or when collected from children under 13 (under COPPA). In some situations, affirmative consent can be impossible or impractical, for example in the context of autonomous vehicles collecting information on passersby; the use of automated license plate readers; biometrics or facial recognition; or Wi-Fi retail analytics. In these situations, other legal obligations apply under different regimes (such as the GDPR), including limits on secondary uses, sharing, profiling, retention, or privacy by design requirements. See Table 1.

Table 1. Legal Protections for Location Data in the US, EU, and Canada

Source of Law	Key Definition (or Text)	Legal or Self-Regulatory Protections
U.S. CONSTITUTION, Fourth Amendment	"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . ."	The U.S. Supreme Court held in *Carpenter v. United States* that location data carries unique sensitivities because of its ability to reveal intimate information about people's behavior, patterns, and personal life. 138 S. Ct. 2206 (2018). Under Carpenter, law enforcement collection of long-term cell site location information (CSLI) requires a warrant.
FEDERAL TRADE COMMISSION ACT, 15 U.S.C. § 45(a) *Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade*	The FTC Act provides that "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." § 45 (a)(1).	The Federal Trade Commission (FTC)'s 2012 Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change" states that companies should obtain **affirmative express consent** prior to collecting sensitive data, and for materially inconsistent uses. Recognizing the "sensitivity of . . . real time location," the FTC urged companies to: • provide prominent notice and choice for consumers where location is shared with third parties; and • implement "privacy by design" including data security, accuracy, and limits on collection, use, transfer, and retention. In 2014, the FTC settled with Goldenshores Technologies, LLC, the creators of a flashlight app, requiring them to obtain affirmative express consent before collecting geolocation information, and to provide disclosures to consumers on when, how, and why their geolocation information was being collected, used and shared. In 2016, the FTC settled with mobile advertising network InMobi for tracking the locations of consumers without their consent, and for failing to respect users' choice not to share location data.

Source of Law	Key Definition (or Text)	Legal or Self-Regulatory Protections
THE COMMUNICATIONS ACT OF 1934 as amended 47 U.S. Code § 222 Privacy of customer information	***"Customer proprietary network information"*** means "information that relates to the quantity, technical configuration, type, destination, **location,** and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship . . ." § 222(h)(1).	Federal telecommunications laws require telecommunications carriers to maintain the confidentiality of individually identifiable customer **proprietary network information (CPNI),** including location information associated with the use of a telecommunications service. § 222(c)(1). In general, CPNI cannot be used or shared outside of providing the service, except with consent. Call location information, in particular, can only be used with "express prior authorization" (§ 222(f)), unless the location data is being used to enable emergency services. § 222(d)(4).
CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA), 15 U.S.C. § 6501(8)(F) *Definitions*	***"Personal information"*** means "individually identifiable information about an individual collected online, including . . . **geolocation** information sufficient to identify street name and name of a city or town." 16 C.F.R. pt. 312.	Under the COPPA Rule (last updated in 2013 through FTC rulemaking), location data is a form of personal information. As a result, location data requires verified parental consent before a company may collect it from children under 13 in the United States. There are limited exceptions to the requirement for parental consent for personal information, such as when a company processes data in limited ways for "internal operations." See the FTC's "Complying with COPPA, Frequently Asked Questions" (COPPA FAQ).
VIDEO PRIVACY PROTECTION ACT (VPPA), 18 U.S.C. § 2710 *Wrongful disclosure of video tape rental or sale records*	***"Personally identifiable information"*** includes information that "identifies a person as having requested or obtained specific video materials or services from a video tape service provider.'" § 2710(a)(3).	Federal courts have taken different approaches to the interpretation of "personally identifiable information" under the VPPA. In 2016, the First Circuit Court of Appeals ruled in *Yershov v. Gannett Satellite Information Network, Inc* that personally identifiable information included the "GPS coordinates of a device," when tied to a unique mobile identifier (such as an Android ID), given "how easy it is to locate a GPS coordinate on a street map . . . [such that the] disclosure would enable most people to identify what are likely the home and work addresses of the viewer."
CALIFORNIA CONSUMER PRIVACY ACT (CCPA), Cal. Civ. Code § 1798.100, et seq. CCPA Regulations § 999.300-337	***"Personal information"*** means information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." § 1798.140(o). Personal information includes, but is not limited to . . . **geolocation.**" § 1798.140(o)(1)(G).	The CCPA defines personal information broadly to include "geolocation data" as well as inferences drawn from geolocation data to create a profile about a consumer. § 1798.140(o). As a result, location data is subject to notice and transparency requirements, and the consumer rights of access, deletion, and opt-out of sale. In the Attorney General's regulations adopted pursuant to CCPA, geolocation from mobile apps is given as an example of a type of personal information that could be used for purposes that a consumer would not reasonably expect: *"For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application . . ."* § 999.315.

Source of Law	Key Definition (or Text)	Legal or Self-Regulatory Protections
THE CALIFORNIA PRIVACY RIGHTS AND ENFORCEMENT ACT OF 2020 ("CPRA") 1798.140. (v)(1)(G); (t); (w); (z); & (ae) *Definitions* 1798.121. Consumers' *Right to Limit Use and Disclosure of Sensitive Personal Information*	***"Precise geolocation"*** 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 one thousand, eight hundred and fifty (1,850) feet, except as prescribed by regulations. § 1798.140(w).	The California Privacy Rights Act (CPRA), passed by ballot initiative in 2020, amends the California Consumer Privacy Act (CCPA). Under the CPRA, California residents will have the right to request that companies limit the use of their sensitive personal information, which includes precise geolocation, to that which is "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services . . ." § 1798.121(a). If a consumer directs a business not to use, share, or sell their sensitive personal information for additional purposes, the business will be prohibited from doing so unless the consumer subsequently provides consent. The business will be prohibited from requesting consent from the consumer for 12-months after a consumer has directed them to limit the use of their sensitive personal information. Limited exceptions exist under the CPRA for "service providers" that process data on behalf of businesses pursuant to a defined "business purpose." § 1798.135(f). Notably, however, precise geolocation may not be used for short-term, transient "non-personalized advertising" to qualify under the CPRA's limited business purposes exception. § 1798.14(t). The substantive provisions of the CPRA become operative in 2023.
NETWORK ADVERTISING INITIATIVE ("NAI") NAI Code of Conduct (2020)	***"Precise Location Data"*** means "information that describes the precise geographic location of a device derived through any technology that is capable of determining with reasonable specificity the actual physical location of an individual or device, such as GPS level latitude-longitude coordinates or location-based radio frequency signal triangulation." § I(l).	Companies that commit to the NAI's Code of Conduct agree to obtain opt-in consent, or reasonable assurances from partners that consent was obtained, prior to collecting precise location data or using it for targeted advertising. Opt-in consent is also required for initially collected location data that has been rendered "imprecise" if the data will be used for Tailored Advertising or Ad Delivery and Reporting, however, subsequent uses do not require opt-in consent. Compliance with the Code is audited by NAI and enforceable by the FTC as a public commitment. In 2020, NAI updated its guidance for members on determining whether location data is "imprecise," including four factors: (1) the area of the identified location; (2) the population density of the area; (3) the accuracy of the data; and (4) presence and detail of the location's timestamp.

Source of Law	Key Definition (or Text)	Legal or Self-Regulatory Protections
DIGITAL ADVERTISING ALLIANCE ("DAA") SELF-REGULATORY PRINCIPLES ("DAA PRINCIPLES"): Mobile Guidance, the Online Behavioral Advertising Principles, the Cross-Device Guidance, and the Multi-Site Data Principles	***"Precise Location Data"*** means "data obtained from a device about the physical location of the device that is sufficiently precise to locate a specific individual or device." Mobile Guidance Principles, § I.(K). Precise location data "may include, for example, data obtained from cell tower or WiFi triangulation techniques, or latitude-longitude coordinates obtained through GPS technology, if such data is sufficiently precise to locate a specific individual or device. . . [and] does not include five-digit ZIP code, city name, general geographic information whether derived from an IP address or other sources . . ." Commentary, Mobile Guidance Principles, § I(K). .	"First-party" companies (app publishers) that commit to the DAA Principles and authorize third-parties to collect precise location data agree to obtain valid consent and to offer "clear, meaningful, and prominent notice" ("enhanced notice") of transfers to third parties for interest-based advertising purposes. First parties must also have a notice of their precise location data practices regarding interest-based advertising, a tool to withdraw consent, and a statement of adherence to the DAA Principles. This notice is usually located in a privacy policy, and a company's enhanced notice typically links to this notice. "Third-party" companies (ad tech companies) that commit to the DAA Principles must also have a notice of their precise location data practices regarding interest-based advertising which includes a description of their practices, a tool to withdraw consent, and a statement of adherence to the DAA Principles. This notice is usually in a privacy policy. Third-party companies commit to getting consent from users for their collection of precise location data for interest-based advertising or getting reasonable assurances from first-party partners that consent was obtained. The DAA Principles are enforced cooperatively by BBB National Programs' **Digital Advertising Accountability Program** and Association of National Advertisers (ANA), as well as enforceable by the FTC as a public commitment.
EU GENERAL DATA PROTECTION REGULATION (GDPR) 2016/679 Art.4 *Definitions* Art.5 *Principles relating to processing of personal data* Art.6 *Lawfulness of processing* Art.22 *Automated individual decision-making, including profiling* Recital 71 *Profiling*	***"Personal data"*** means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, ***location data,*** an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Art. 4(1). ***"Profiling"*** means "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, **location or movements**." Art. 4(4).	In the EU, location data is subject to the GDPR's broadly applicable requirements of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. Art. 5. In order to collect location data, a company must rely on one of six lawful bases: affirmative consent from the individual, performance of a contract, compliance with a legal obligation, protection of a person's vital interests, public interest, or legitimate interests. Art. 6. In certain cases, limited processing of location data is permitted in the EU on the basis of "legitimate interests," for example, in cases involving Wi-Fi analytics when data is processed subject to strict retention limits and anonymization. See, e.g., Conseil d'État, Decision of 08.02.2017, "JCDecaux France" (Fr) (*See* unofficial translation) (a case involving the tracking of mobile phones through WiFi-connected street furniture). Profiling is permitted under the GDPR if it does not lead to solely automated decisionmaking in furtherance of legal or similarly significant effects. Art. 22. Profiling based on location data may require affirmative consent (rather than, for example, a "legitimate interests" lawful basis) if the profiling is particularly intrusive or involves tracking of

Source of Law	Key Definition (or Text)	Legal or Self-Regulatory Protections
		individuals across multiple locations. See European Data Protection Board (EDPB), Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2016) (describing the elements of profiling).
CANADA'S PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA), S.C. 2000, c 5 § 2(1) *Definitions*	***"Personal information*** means information about an identifiable individual." § 2(1).	Canada's PIPEDA requires organizations to comply with broadly applicable fair information principles for processing personal information, including consumer rights to access and correct data; and limitations on the collection, use, disclosure, and retention of personal information. See Office of the Privacy Commissioner of Canada (OCP), PIPEDA in Brief (May 2019). Under PIPEDA, data is capable of constituting "personal information" if it is "about an identifiable individual." § 2(1). This has been interpreted in public statements by the Office of the Privacy Commissioner of Canada (OCP) to include geolocation data, as it "can reveal information about the habits and activities of individuals, for example, medical visits or places that they regularly frequent." *See* News Release, *Privacy Commissioners Launch Joint Investigation into Tim Hortons Mobile App* (GATINEAU, QC, June 29, 2020). In 2011, the OCP found that personal information included "[t]racking information collected from a Global Positioning System (GPS) placed in company vehicles . . . since the information can be linked to specific employees driving the vehicle." *PIPEDA Case Summary #2006-351.* In 2020, the OCP launched an investigation into Tim Hortons' collection of geolocation data from their consumer-facing mobile app, to look into "whether the organization is obtaining meaningful consent from app users to collect and use their geolocation data for purposes which could include the amassing and use of detailed user profiles, and whether that collection and use of the data is appropriate in the circumstances."

ADDITIONAL RESOURCES

Future of Privacy Forum, "Understanding the 'World of Geolocation Data'" (May 2020)

MIT Media Lab, "The Tradeoff Between the Utility and Risk of Location Data and Implications for Public Good" (December 2019)

Article 29 Data Protection Working Party, "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679" (Adopted February 2018)

Information Commissioner's Office, "Wi-Fi Location Analytics" (February 2016)

Network Advertising Initiative, "Guidance for NAI Members: Determining Whether Location is Imprecise" (July 2015)

Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers" (March 2012)

Teresa Scassa & Anca Sattler, "Location-Based Services and Privacy" Canadian Journal of Law and Technology (June 2011)

Article 29 Data Protection Working Party, "Opinion 13/2011 on Geolocation Services on Smart Mobile Devices" (Adopted May 2011)

Future of Privacy Forum (FPF) is a 501(c)(3) non-profit organization based in Washington, DC that supports privacy leadership and scholarship in support of emerging technologies.

Contact the authors:

Stacey Gray, Senior Counsel, sgray@fpf.org

Pollyanna Sanderson, Policy Counsel, psanderson@fpf.org

1400 Eye Street, NW, Suite 450
Washington, DC 20005

fpf.org