imageBROKER/Alamy Stock Photo

Using Geolocation Data in Litigation

With the rise of smart phones and wearable devices, the use of applications (apps) with geolocation features has increased exponentially in recent years, and has gained even more prominence since the introduction of contact tracing through the ongoing COVID-19 pandemic. Besides offering many conveniences and benefits to users in their daily lives, geolocation features can provide important information for various types of litigation. Counsel bringing or defending a claim should consider whether and how to employ geolocation data to support their case and must understand the unique issues that using geolocation data in litigation presents.

SAMANTHA V. ETTARI
SENIOR COUNSEL
PERKINS COIE LLP

Samantha's extensive experience in privacy, data security, and data management issues includes legal, practical, and reputational risk counseling, often in the context of mergers, acquisitions, and technology-driven strategic and investment transactions. As senior counsel at the firm, she advises clients on both domestic and international privacy statutes and regulations, as well as cross-border transfers of data. Samantha is also a seasoned litigator and trial lawyer and has litigated diverse matters to final judgment, including contract and licensing disputes and false advertising and consumer fraud claims.

Geolocation data refers to information derived from an electronic device, such as a mobile phone, tablet, vehicle receiver, or laptop, that can reveal the precise location of that device and, presumably, the individual using the device. Apps with tracking or geolocation capabilities are increasing in popularity and notoriety. Geolocation features on an app may, among other things:

- Provide information regarding the local weather and nearby restaurants, gas stations, hotels, and parks.
- Give directions to a destination and the expected time of arrival based on traffic flows and the user's movement, and guide a user through a building from room to room.

- Allow a user to track the locations of other individuals, such as the location of a specific student or faculty employee on a densely populated campus.
- Track a user's running distance, time, pace, and route.

Geolocation data is generally obtained through:

- Global Positioning System (GPS) satellite-based navigation.
- Bluetooth technology.
- Cell site location information (CSLI).
- Crowd-sourced WiFi hotspot data.
- WiFi towers.

If an app's location services are turned on, geolocation data can be collected even when the app is not in active use. Mobile devices with cell service also constantly scan the area for the nearest cell site and ping the device's location every seven to nine minutes, regardless of whether the device or any loaded app is in use, creating CSLI that is usually stored with the cell service provider.

Given the proliferation of geolocation-based mobile apps, as well as the substantial volume of information constantly being generated and collected, geolocation data is becoming an important focus in litigation where a user's location is relevant to the dispute. Counsel should become familiar with this evolving technology and area of law and understand the key issues and considerations surrounding the use of geolocation data in litigation, including:

- How geolocation data is stored and accessed.
- The privacy issues raised by geolocation data.
- How geolocation data may be used in particular types of cases.
- How to address and obtain geolocation data during discovery.
- What to do with geolocation data at the conclusion of a litigation.

STORAGE OF AND ACCESS TO GEOLOCATION DATA

Depending on the nature of a specific app or device, geolocation data may be stored on:

- **The device itself.** A forensic image of a mobile device often captures some geolocation data from various sources, including communication apps and photographs that may contain metadata, such as where the photograph was taken. However, given that memory space on a small mobile device is limited, the data may be periodically auto-deleted without user notice or control. (For resources to help counsel preserve documents and electronically stored information (ESI), search Preserving Documents and Electronically Stored Information Toolkit and Litigation Hold Toolkit on Practical Law.)
- **Company servers.** Some apps store geolocation data on the app provider's company servers. The apps may allow users to view the data and download it to the device themselves, or allow the provider to do so on request. Similarly, operating system providers, such as Microsoft, Apple, and Google, contain and store geolocation data on their servers. Apart from collecting geolocation data to deliver certain app features, a secondary market has developed to use the data to compile information about the tracked individual to predict consumer habits and to sell and profit from this information.

Once accessed, geolocation data may appear in a plain text (.txt) or an Excel (.xls) file format. E-discovery vendors often have tools that can make the information more visually accessible and functional for use in litigation.

PRIVACY ISSUES RAISED BY GEOLOCATION DATA

As privacy laws continue to expand across the globe, certain statutes and regulations have identified geolocation data as information that requires protection, including notice from those who collect it and allowing use of the data only with a legal basis set out in the applicable statute. Examples include:

- **The California Consumer Privacy Act (CCPA).** The CCPA, which creates a private right of action for consumers in the context of data breaches, lists geolocation data as personal information. Geolocation data can therefore trigger the CCPA's data subject rights and multiple disclosure, collection, and sale obligations (Cal. Civ. Code §§ 1798.140(o)(1)(G), 1798.150(a)). (For more information on the CCPA, search Understanding the California Consumer Privacy Act on Practical Law.)
- **The EU General Data Protection Regulation (GDPR).** The sweeping GDPR (Regulation (EU) 2016/679), which has broad extraterritoriality provisions, lists "location data" under the personal data definition. Geolocation data can therefore trigger the GDPR's data subject rights and data protection, disclosure, collection, use, and transfer obligations (GDPR, Art. 4(1)). (For more information on the GDPR, search GDPR Resources for US Practitioners Toolkit on Practical Law.)

To date, litigation concerning the privacy implications of geolocation data has mainly arisen in the context of:

- Civil consumer class actions.
- Criminal pretrial suppression motions.

CIVIL CLASS ACTIONS

In recent years, there have been numerous civil class action lawsuits concerning the undisclosed collection or misuse of private geolocation data. For example, in *Greenley v. Avis Budget Group Inc.*, the plaintiff alleged that a car rental company impermissibly collected and stored his private information through the pairing of the plaintiff's mobile phone to the rental vehicle, in violation of the California Constitution and certain California consumer privacy statutes. Specifically, the plaintiff alleged that the pairing allowed the rental vehicle to improperly collect, copy, and transfer information from the device to the vehicle's GPS technology and automotive infotainment systems, and that the data was retained unless and until there was a manual purge. However, the court granted the defendant's motion to dismiss, holding that the plaintiff failed to allege a sufficiently concrete injury

to establish Article III standing, and remanded the case to state court. (2020 WL 5230471, at *1-2, *4-5 (S.D. Cal. Sept. 2, 2020).)

Similarly, there has been an increase in civil class action lawsuits brought against operating service providers. For example, in *In re iPhone Application Litigation*, the plaintiffs brought various privacy claims against Apple and other defendants, alleging that the defendants' conduct violated the California Constitution, the Stored Communications Act (SCA) (which creates civil and criminal liability for certain unauthorized access to stored communications and records), and other statutes. The plaintiffs argued that Apple violated their privacy rights by allowing third party apps to collect and use their geolocation data without their consent, and that Apple continued to monitor and store their geolocation data even when the user had disabled the geolocation feature. (844 F. Supp. 2d 1040, 1049-51 (N.D. Cal. 2012).)

The *In re iPhone Application Litigation* opinion noted that "computer systems of an email provider, a bulletin board system, or an [internet service provider] are uncontroversial examples of facilities" through which electronic services are provided within the meaning of the statute. However, a key question was whether a single "individual's computer, laptop, or mobile device fits the statutory definition." In dismissing most of the plaintiffs' claims, the court determined that the plaintiffs failed to allege that the iOS devices constituted a facility under the SCA. Further, the court noted that the disclosure of geolocation data to third parties was not "an egregious breach of social norms" that would violate California's constitutional right to privacy. (844 F. Supp. 2d at 1049, 1056-60, 1063.)

By contrast, in *Cousineau v. Microsoft Corp.*, another court applied a technologically evolving meaning to the term "facility" to conclude that it can encompass an individual's mobile device. In that case, the plaintiffs alleged that Microsoft collected and stored their geolocation data on its servers and on the devices themselves, and that Microsoft impermissibly used the data it collected to improve its geolocation services and drive targeted advertising based on the users' location. The court held that the plaintiffs stated a plausible claim for misuse of geolocation data under the SCA, but it dismissed the plaintiffs' claims under the Wiretap Act and state privacy statutes. (992 F. Supp. 2d 1116, 1119, 1121, 1124-25, 1130 (W.D. Wash. 2012); see also *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 817, 822, 824, 831 (N.D. Cal. 2020) (dismissing with leave to amend Google Assistant users' claims for violation of the Wiretap Act and the California Constitution, as well as for unauthorized access under the SCA (18 U.S.C. § 2701(a)), but finding that the plaintiffs stated a claim for unlawful disclosure under the SCA (18 U.S.C. § 2702(a))).)

As privacy concerns continue to grow, statutes such as the SCA, or new statutes and regulations, may provide consumers with redress for the undisclosed collection or misuse of their geolocation data. Counsel can expect to see more privacy-related litigation against device manufacturers, app developers, and app providers due to the increasing use of geolocation data.

CRIMINAL MOTION PRACTICE

In the criminal context, defendants have sought to exclude geolocation evidence on the basis that it violates their Fourth Amendment right to a reasonable expectation of privacy. In *Carpenter v. United States*, the US Supreme Court held that:

- Individuals have a reasonable expectation of privacy regarding their physical movements captured through geolocation techniques, regardless of whether the government employs its own surveillance technology or leverages the technology of a wireless carrier.
- The government's collection of the plaintiff's geolocation data constituted a "search" under the Fourth Amendment. Therefore, the government was required to obtain a search warrant supported by probable cause before collecting the data.

The Supreme Court noted that the standard applicable to the court order obtained by the government before it collected the geolocation data fell "well short of the probable cause required for a warrant." (138 S. Ct. 2206, 2217, 2221 (2018).)

Following *Carpenter*, police and investigators have included more detailed information in support of their applications to obtain a suspect's geolocation data (see, for example, *United States v. Palazzola*, 2020 WL 4474147, at *1 (E.D. Mich. Aug. 4, 2020); but see *People v. Yaguchi*, 62 Misc. 3d 1054, 1063 (Sup. Ct. Bronx Co. 2019) (stating that the defendant, a veteran of the Bronx police department, had no expectation of privacy in an employer-issued device, including the geolocation data in it)).

USE OF GEOLOCATION DATA IN PARTICULAR TYPES OF CASES

As geolocation technology improves, the practical uses of geolocation data in litigation is certain to increase. This data can be used to both build and defend claims and to help establish jurisdiction.

CASE EXAMPLES

Examples of the types of cases in which counsel should consider geolocation data to support a party's arguments include:

- **Wrongful termination.** Where a mobile or remote employee (who is lawfully tracked by the employer) has alleged wrongful termination, the employer may use geolocation data to demonstrate that the termination was based on, for example, the employee's failure to adhere to assigned routes or attend customer appointments on time (see, for example, *Edwards v. 4LJ, L.L.C.*, 2020 WL 5229686, at *2 (5th Cir. Sept. 2, 2020) (case in which GPS location data was relevant to a Fair Labor Standards Act litigation concerning bonuses and compensation rates); *Sanchez v. M&F, LLC*, 2020 WL 4671144, at *7-8 (M.D. Fla. Aug. 12, 2020) (employment dispute about overtime wages in which GPS location data was litigated); *Crossman v. Carrington Mortg. Servs., LLC*, 2020 WL 2114639, at *1, *5 (M.D. Fla. May 4, 2020) (a wrongful termination and discrimination action in which

the defendants sought geolocation data among other ESI in discovery and the court ordered its production)). (For more information on employee terminations, search Employee Termination: Best Practices on Practical Law.)

- **Personal injury.** Where an injured plaintiff alleges the inability to leave home due to the injury, geolocation data from the plaintiff's fitness apps can provide evidence of the plaintiff's physical activity outside the home (for example, daily walks or runs in a nearby park) to use in defending the case (see, for example, *Jalowsky v. Provident Life & Accident Ins. Co.*, 2020 WL 4814286, at *2 (D. Ariz. Aug. 17, 2020) (compelling production of information concerning fitness tracking devices and software used by a plaintiff in disability litigation alleging serious, permanent physical injuries)). This type of information may be used for similar purposes in a wrongful death action (see, for example, *Estate of Rand, Administrator v. Lavoie*, 2017 WL 11541229, at *2, *5 (D.N.H. July 25, 2017) (holding that the content of the decedent's Garmin watch, including geolocation data, was discoverable)).
- **Trade secrets.** Where an employer alleges that an employee accessed highly confidential data or prototypes that the employee did not have permission to view, the employer may use geolocation data to prove the employee's presence in restricted areas with access to that data or device. An employer or a competitor may also use geolocation data where the data is the trade secret itself. (See, for example, *McDonald Apiary, LLC v. Starrh Bees, Inc.*, 2016 WL 5921069, at *3 (D. Neb. Oct. 10, 2016) (holding that a jury could reasonably find that a database of beehive locations was a trade secret).) (For more information on trade secrets, search Trade Secrets Litigation and Protection of Employers' Trade Secrets and Confidential Information on Practical Law.)
- **Matrimonial actions.** Where one spouse alleges that the other spouse dissipated marital assets on dinners, vacations, and travel with another individual, geolocation data from photographs or other apps may help establish the offending spouse's presence at those locations with the other individual, while geolocation data from the apps of the spouse asserting the claim may help establish that spouse's absence from those locations (see, for example, *Resnik v. Coulson*, 2019 WL 2256762, at *1 (E.D.N.Y. Jan. 4, 2019) (describing a state court order in an ongoing divorce proceeding that required the parties to preserve all of their ESI)). Geolocation data may be relevant to custody disputes as well.
- **Copyright infringement.** Where unknown defendants have impermissibly and illegally downloaded or distributed copyrighted content, counsel may need to use geolocation data to establish jurisdiction over them (see, for example, *Strike 3 Holdings, LLC v. Doe*, 2019 WL 1778054, at *2 (D.D.C. Apr. 23, 2019); see below *Establishing Jurisdiction*). Geolocation data may also be relevant to a substantive trademark or copyright infringement litigation (see, for example, *Superior Consulting Servs., Inc. v. Shaklee Corp.*, 2017 WL 8893863, at *4 (M.D. Fla. July 27, 2017)). (For more information on copyright infringement, search Copyright Infringement Law Toolkit on Practical Law.)

ESTABLISHING JURISDICTION

As noted above, geolocation data may be used to establish a court's personal jurisdiction in litigation. In federal court, parties generally may not engage in discovery until all parties have appeared and participated in required discovery planning. However, litigants sometimes require discovery to identify another party. In this circumstance, a party may petition the court to conduct targeted discovery and demonstrate its "good faith belief that such discovery will enable it to show that the court has personal jurisdiction over the defendant" (*Strike 3 Holdings, LLC*, 2019 WL 1778054, at *1).

For example, a petitioning party can use the unknown party's geolocation data, including its IP address, to show that the unknown party likely resides (or that the injury likely occurred) in a particular location for purposes of establishing the court's personal jurisdiction. The party may then seek to obtain discovery from the unknown party's internet service provider (ISP) to determine the unknown party's identity. This situation often arises in the context of copyright infringement litigation (see, for example, *Strike 3 Holdings, LLC*, 2019 WL 1778054, at *1-2 (stating that geolocation data provided a basis for showing the defendant's location to establish personal jurisdiction and allowing the plaintiff to propound discovery on an ISP before the Rule 26(f) conference to determine the defendant's identity); *Malibu Media, LLC v. Doe*, 2015 WL 5173890, at *1-2 (D.D.C. Sept. 2, 2015); *Nu Image, Inc. v. Does 1–23,322*, 799 F. Supp. 2d 34, 41-42 (D.D.C. 2011); but see *AF Holdings, LLC v. Does*, 752 F.3d 990, 996 (D.C. Cir. 2014) (denying the plaintiff's pre-complaint request for discovery, in part because the discovery sought was not narrowly tailored to identify parties in the relevant jurisdiction)).


Search Commencing a Federal Lawsuit: Initial Considerations for more on personal jurisdiction.

OBTAINING GEOLOCATION DATA DURING DISCOVERY

Parties that seek to obtain geolocation data in civil litigation commonly do so during the discovery phase. Federal Rule of Civil Procedure (FRCP) 34 allows discovery of certain ESI, including "data or data compilations," which encompasses geolocation data. However, under FRCP 26(b), counsel should limit discovery to relevant information that is proportional to the needs of the case, taking into account whether the information is not reasonably accessible because of an undue burden or cost.


Search Making and Responding to Proportionality Objections for more on proportionality-based objections in federal civil discovery.

If geolocation data is important to the litigation, counsel should:

- Assess all potential and proportional sources of geolocation data relevant to the litigation and in the possession, custody, and control of the adversary and the client (for more information, search Possession, Custody, and Control of ESI in Federal Civil Litigation on Practical Law). Additionally,

counsel should consider whether to seek discovery of geolocation data in a third party's possession, custody, and control (for a sample document preservation letter to a third party, with explanatory notes and drafting tips, search Document Preservation Letter for a Nonparty on Practical Law).

- Discuss geolocation data retention and collection with the client, making sure to address:
  - the client's own relevant geolocation data in the possession of others that legally may be in the client's possession, custody, or control; and
  - disabling auto-delete features or conducting early forensic collection.

  (See, for example, *Edwards*, 2020 WL 5229686, at *2 (case in which an employer mistakenly believed it did not have access to location data but ultimately determined that the data was accessible after the court levied sanctions for its failure to produce the data).)
- Explicitly include geolocation data in a preservation letter to the adversary, including:
  - detailed instructions for disabling auto-delete features; or
  - a specific request that a mobile device be forensically imaged to preserve whatever geolocation data remains on the device (in case the device has an auto-delete feature that cannot be disabled by the user).

  (See, for example, *Sanchez*, 2020 WL 4671144, at *7 (noting that certain text messages and GPS locations used to generate records in the form of spreadsheets were temporary and self-erasing and therefore not recoverable during the litigation).) (For a sample preservation letter, with explanatory notes and drafting tips, search Document Preservation Letter for an Opposing or Co-Party on Practical Law.)
- Flag the geolocation data source early for the adversary and the court at the Rule 26(f) and compliance conferences. Given that it is a relatively new type of data source, courts and adversaries might be unfamiliar with the existence, accessibility, and retention of geolocation data.
- Propound written discovery requests and interrogatories that include detailed and specific requests for geolocation data or seek information concerning the availability and accessibility of geolocation data (for resources on document requests and interrogatories, search Document Discovery Toolkit and Interrogatories Toolkit (Federal) on Practical Law). In doing so, counsel should:
  - specify the production format for responsive geolocation data (and other ESI), so that the information received is useful; and
  - consider consulting with an e-discovery vendor (or in-house litigation technologist) to ensure that the format request is compatible with the document review platform and will encompass any relevant metadata sought.
- When defining "Documents" or "Electronically Stored Information" in discovery requests:
  - include "geolocation data," "location data," "GPS data," and "tracking data" in the definition; and
  - consider identifying specific apps that could reasonably be expected to contain geolocation data relevant to the dispute.

  (For a collection of resources to help counsel and litigants meet their e-discovery obligations, search E-Discovery Toolkit on Practical Law.)
- Consider whether to put in place a protective order or confidentiality agreement to protect the use of the geolocation data during the litigation, specifying:
  - who can view and access the data;
  - whether parties must redact certain data in public filings to protect individuals' movement and locations from public access;
  - which privacy regulations may apply; and
  - how and when the parties will return data to the producing party or destroy the data.

  (For more information, search Protective Orders: Overview (Federal) and Confidentiality Agreement (Order) (Federal) on Practical Law.)
- Consider engaging a technology or forensic consultant to assist in understanding the geolocation data and how best to present it visually, and to ensure the data's admissibility when using it in dispositive motions, discovery motions, and at a hearing or trial (for more information, search E-Discovery: Authenticating Electronically Stored Information and Questions to Ask a Prospective E-Discovery Vendor Checklist on Practical Law).
- Make sure that the litigation team understands how to speak generally about the data source and its collection, use, and relevance to the dispute.

Counsel should also consider the legal boundaries for gathering geolocation data. For example, counsel should ensure that app providers, forensic investigators, or others do not impermissibly use or hack into a user's device, illicitly install spyware to capture geolocation data, or turn on tracking features without the user's notice or consent. Numerous ethics decisions and articles address the impermissible collection of data, including geolocation data (see, for example, American Bar Association, Forensic Examination of Digital Devices in Civil Litigation: The Legal, Ethical and Technical Traps (Mar. 1, 2016), available at *americanbar.org*).

RETURN OR DESTRUCTION OF GEOLOCATION DATA

As with all sensitive data, in addition to establishing clear parameters around the data's use and disclosure during the litigation, provisions for the return or destruction of the data at the conclusion of the litigation should be set out in writing and enforced.