PAUL HASTINGS

STAY CURRENT

April 2020

Follow @Paul_Hastings

PH COVID-19 Client Alert Series: Location Privacy in a Crisis—Considerations for Businesses

By Sherrese Smith, Aaron Charfoos & Andrew Erber

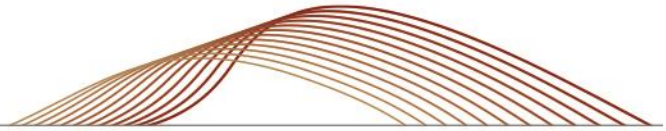
The fight against COVID-19 has gone mobile. Israel has approved emergency regulations to use smartphone location histories to warn people about potential COVID-19 exposure and enforce self-quarantines. South Korea's epidemiological surveys are using individual GPS data to confirm interview details and notify the public of confirmed cases through mobile alerts. There are press reports of the Trump Administration exploring the value of location data in combating the spread of the virus.

These initiatives bring new tools to public health officials' fight against COVID-19. But privacy concerns are at their zenith when location is involved. Geo-tracking data is notoriously difficult to anonymize and often trivial to re-identify. A simple search of public property records is typically enough to link GPS data to an individual.

Debates in the press over government geo-tracking also have the potential to heighten scrutiny of businesses that leverage location data. Recently, the major U.S. wireless carriers became the target of an FCC investigation into third-party data sharing arrangements involving customer location data. The Commission has proposed fines of over $200 million for alleged violation of the Communications' Act—a clear warning sign that regulators are taking location privacy seriously.

With the world being re-shaped by COVID-19 and location data at the forefront of public policy, companies should take this time to engage in self-assessments and look with fresh eyes at their use of location data. Geo-tracking smart devices is an essential value add to many businesses—including foot-traffic analysis for retailers, geo-fenced emergency alerts and local news highlights in the media sector, and traffic-pattern optimization for personal vehicles and commercial delivery fleets. We recommend that companies keep four principles in mind when conducting such privacy assessments.

- **Know Your Data.** Aligning privacy interests with enterprise risk requires mapping and categorizing the data your company holds. Location data comes in many forms—ranging from precise GPS coordinates to aggregate, de-identified "heat maps". The more precise the data, the higher the privacy risk, so it's critical to know which elements you have and where they come from. With GDPR enforcement in full swing (and CCPA enforcement and other state regulations on the horizon), companies need to know their data well.



- **Privacy By Design.** Workflows and projects that involve location data should be designed with privacy in mind. Data minimization is critical to this process. Asking how your company can reduce (or eliminate) the retention of location data can vastly reduce the sensitivity of data sets and privacy concerns.

- **Third-Party Use and Contract Hygiene.** Establish clarity with vendors and other third parties on the use, processing, and retention of location data. If sourcing location data from a vendor, obtain commitments from the vendor that the data was collected legally and seek indemnification for any issues. Specify in writing the data elements to be shared and double-check that data sets comply with contractual standards.

- **Privacy Policies.** If collecting the data yourself, ensure that your privacy policy is robust, opt-in and opt-out mechanisms are clear, and that uses are restricted to those disclosed in the policy. The major mobile operating systems all provide robust location control features, so use them. Provide meaningful notice to data subjects and honor their requests to delete or access their data.

The regulatory landscape governing the collection, use, and sharing of location data is changing rapidly, and businesses need to be prepared for tightening of consent and sharing standards in the future. The attorneys and experienced consultants in our Privacy and Cybersecurity practice group help clients navigate these issues every day. We are available and ready to help you navigate the privacy landscape in this time of unprecedented change and uncertainty.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Washington, D.C.

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Atlanta

Andrew J. Erber
1.404.815.2289
attorney@paulhastings.com