ALSTON & BIRD

Privacy Advisory:

Location and Mobile Data in the Fight against COVID-19: What to Expect in the U.S. and Around the Globe

April 13, 2020

Location and Mobile Data in the Fight against COVID-19: What to Expect in the U.S. and Around the Globe

by Amy Mushahwar, Daniel Felz, and Jon Knight

* * * * * *

Governments are increasingly seeking to leverage consumer geolocation and other mobile device data to assist with fighting the spread of COVID-19, as cases continue to mount globally. Location data can be of significant value to public health models, such as models that determine areas where social-distancing measures are needed or test whether such measures are effective. In some areas, governments are also using location data for contact tracing, or for measures designed to monitor and enforce quarantine of individuals who have tested positive for COVID-19 or those with whom such persons have come into contact.

Given the urgency of this matter, nations are now using some variant of location data for policymaking or protective measures. Even traditionally privacy-protective jurisdictions such as Austria, Germany, Italy, and the UK have found methods – reportedly approved of by privacy regulators – for leveraging anonymized mobile location data in the fight against COVID-19. This data will likely continue to be important as COVID-19-related restrictions are lifted, and governments attempt to monitor public health as individuals gradually return to pre-COVID economic activities.

Telecommunications providers and other technology companies have vast stores of location data that can provide significant value in these efforts. Not surprisingly, governmental authorities around the world have been approaching businesses in these sectors to gain access to location data assets. Making location and other mobile device data available to governmental agencies can also raise significant data protection issues for the companies involved.

This Advisory briefly summarizes how the United States and other nations are leveraging or considering using location and other device data to fight COVID-19.

1. United States – A Timeline of Our Measures

- **Initial Discussions.** In mid-March, press reports that the federal government had contacted technology companies to discuss using location data to combat COVID-19 prompted Senator Ed Markey to publish a letter asking the administration to provide answers about how location data would be used. Around the same time, scientists, technologists and epidemiologists published an open letter in support of leveraging mobile data against COVID-19.

- **Funding for CDC Data Efforts in Stimulus Bill.** Congress's stimulus bill (the CARES Act), signed into law on March 27, requires the CDC to develop data-driven COVID-19 solutions. In particular, it appropriates $500 million to the CDC for "public health data surveillance and analytics infrastructure modification." The CDC has 30 days to report to Congress on its "development of a **public health surveillance and data collection system for coronavirus**" using this $500 million in appropriated funds.
    - In using the word "surveillance" to describe this data grant, Congress appears to recognize the importance of contact tracing to the control and prevention of infectious disease. Also, in connection with this authorization on "public health surveillance," it is useful to note that the term "surveillance" has been used for many decades in a different context for public health purposes than for government intelligence activities. For instance, the World Health Organization states: "Public health surveillance is the continuous, systematic collection, analysis and interpretation of health-related data needed for the planning, implementation, and evaluation of public health practice." The CDC has a similar definition (examples of which can be seen in what the CDC describes as its weekly "surveillance report," named "COVIDView").
    - The CARES Act does not limit the types of data the CDC should use for such a program, or how the CDC should obtain it. Mobile location data would potentially be one type of data the CDC could choose to use to fulfill its obligations. The CDC's level of funding would permit significant internal and external efforts, perhaps including collaboration with telecom and/or technology companies.
- **White House Statements.** On April 8, press reports indicated that White House officials were seeking to create a national COVID-19 surveillance system, prompting Sen. Ed Markey to publish a statement indicating he intends to "call[] on the White House to provide more details of this effort." While we have seen no official reports on the status of White House efforts, on April 9, Vice President Pence also stated during a Coronavirus Task Force Press Briefing that the administration is working on both diagnostic virus testing and "surveillance testing," the latter of which will require data to know to know those who may have come into contract with infected individuals.
- **Senate Hearings.** On April 9, the U.S. Senate Committee on Science, Commerce and Transportation held a "paper hearing" titled "Enlisting Big Data in the Fight Against Coronavirus." Witnesses included academics, privacy advocates, and industry representatives. The committee posted the chairman's and ranking member's opening statements and witness testimony. Member questions were sent to witnesses by close of business on April 9, and witnesses have a 96-business-hour turnaround time to answer them. The questions and witness responses will be posted on the committee's website once received and the committee will provide an official transcript for the record.

- **John's Hopkins Tracing Proposal.** On April 13, the Johns Hopkins Center for Health Security issued a National Plan To Enable Comprehensive COVID-19 Case Finding And Contact Tracing In The US. This plan, developed by public health experts in consultation with technologists, identifies three primary needs: (1) rapid testing for all symptomatic cases or those with a reasonable suspicion of COVID-19 exposure; (2) widespread antibody testing; and (3) a technical solution that traces all contacts of reported cases. It proposes, among other things, using a mobile contact-tracing app that could, with user permission, record and store location data for contact tracing and tracking purposes, then sync this data with existing electronic health records. The plan does not contain any specific app technology, instead discussing apps developed in Singapore and the UK (discussed below) as potential examples.

- **Actions by Technology Companies**. A number of technology companies have announced key partnerships and individual actions to aid in COVID-19 data efforts. A few examples include:

  Key Partnerships:

  - Apple & Google: On April 10, Apple and Google announced a partnership on COVID-19 initiative to develop APIs and operating system-level technology to assist in contract tracing. The companies plan to do a two-stage implementation: Stage 1 will enable interoperability between Android and iOS devices using public health authority apps (many of which have been developed to help fight COVID-19, and are explained in detail below). Stage 2 will involve working together to create a broad Bluetooth-based contact tracing platform. The companies have committed to making privacy, transparency, and consent central within these efforts. They have also released their draft Bluetooth specification, cryptography specification, and framework API documentation to the public.

  - COVID-19 Mobility Data Network: A "network of infectious disease epidemiologists" recently launched the "COVID-19 Mobility Data Network" "in partnership with Facebook, Camber Systems, and Cuebiq." These companies provide "aggregated data sets" for epidemiologists to use to "provide situation reports to decision-makers who are implementing social distancing interventions," including reports on effectiveness, high-risk zones, and areas for potential roll-backs.

  Individual Actions:

  - Unacast announced it was launching "a pro bono Covid-19 Toolkit to help public health experts, policy makers, academics, community leaders, and businesses," the first element of which is a "Social Distancing Scoreboard" for all U.S. states and their counties.

  - Facebook also announced it is expanding its "Data for Good" initiative to use "aggregated data" to provide COVID-19-related tools for policymakers, such as "co-location maps," "movement range trends," and "social connectedness" insights.

- Google announced it is providing "mobility reports" for COVID-19 efforts, which use "aggregated, anonymized sets of data from users who have turned on" their "location history" setting to show "movement trends over time by geography."

2. Global Efforts

Outside of the United States, a number of countries have begun to leverage mobile device information in their fight against COVID-19. In many of these countries, collaboration is occurring directly between scientists, technology companies, telecommunications providers and government agencies.

a. The European Approach: Within Europe, telecoms have begun collaborating with government agencies to enable policymakers to use mobile phone location data in COVID-19 prevention. Germany appears to have been the first, with Deutsche Telecom announcing that its affiliate Motionlogic was sharing anonymized signals data with the Robert Koch Institute (Germany's CDC-like public health agency). In Austria and Italy, telecoms have publicly stated they are providing analytics to governments based on anonymous mobile phone data, with Austria's A1 and Italy's Vodafone confirming this collaboration in press releases. In France, a leading public health research institute announced collaboration with telecom Orange. In the United Kingdom, following press reports that telecoms were considering providing mobile data to the government, the UK's privacy regulator publicly stated support for using "anonymized and aggregated" location data to fight COVID-19. Additionally, the UK's National Health Service announced it is working with Microsoft, Amazon Web Services, Palantir, and Faculty AI to develop a visibility solution to manage hospital capacity and resources across the NHS's hospitals. At the pan-European level, the European Commission announced it had conferenced with the "CEOs of European telecommunication companies" to discuss "the sharing of anonymized metadata for modelling and predicting the propagation of the virus" in a manner "that is fully compliant with the GDPR and ePrivacy legislation."

- While in some of the above cases it is difficult to determine with precision, the initial wave of European collaboration likely relies on some version of telecoms sharing anonymized mobile phone information, or models based thereon, to help governments understand the spread of COVID-19, thereby helping policymakers design and implement preventive measures. There appears to be high-level agreement across European democracies that this kind of collaboration can represent a reasonable and effective response to the COVID-19 crisis. Both the European Data Protection Board and European Data Protection Supervisor issued initial statements approving of such collaboration in principle, on conditions that data being shared are anonymous, and administrative controls are in place (such as only limiting access to appropriate experts, implementing strong security, and limiting retention periods). In Germany, the head of Germany's federal privacy regulator publicly tweeted his approval of Deutsche Telekom sharing data with Germany's public health agency. Thus far, the only regulator to publicly take a contrary position has been the Dutch privacy supervisor, which

argued that it is "not possible" to irreversibly anonymize location data, and thus sharing of such data by telecoms requires a new statute. The European Data Protection Board has prioritized providing further guidance on the "use of location data and anonymization of data," and requested a mandate from its plenary to provide such guidance. In parallel, the European Commission has stated it is working with EU Member States to develop a technology toolbox containing a "common approach for the use of anonymized and aggregated mobility data" for COVID-19 modeling, as well as for evaluating social distancing measures.

- Going forward, there may be a "second wave" in which European governments facing particularly severe COVID-19 outbreaks may possibly seek to use mobile phone data for "containment" measures, such as (a) "contact tracing" (i.e., to determine who has been in contact with COVID-diagnosed individuals), or potentially for (b) enforcement of quarantine and social-distancing measures. These uses may go beyond anonymized data sets and require device-level data, and are likely to require further legal discussions. Italy has been one of the hardest hit by COVID-19 in Europe, and in recent interviews, the head of Italy's privacy regulator indicated that contact-tracing and quarantine-enforcement measures would potentially be permissible on an extraordinary and temporary basis under existing laws using health-related mobile apps. His stated rationale was that even the right to privacy is subject to limitations in the face of the collective interest, which can be crafted proportionately, with minimized information collection and subject to appropriate controls.

- The European Commission appears to agree that mobile apps are a promising solution for combatting COVID-19 in a privacy-preserving manner. On April 8, the Commission published a "Recommendation on a Common Union Toolbox for the Use of Technology and Data to Combat and Exit from the COVID-19 Crisis." This Recommendation recognizes that mobile apps "can support health authorities" in "containing the ongoing COVID-19 pandemic," and announces that the Commission will coordinate with Member States to publish a "pan-European approach for COVID-19 mobile applications" by April 15. Under the Commission's Recommendation, the European Data Protection Board and European Data Protection Supervisor will be integrated into any European approach for COVID-19 app development.

b. **AsiaPAC Approaches**: Within Asian nations, governments are using individually identifiable mobile phone data to map movements of COVID-positive individuals, conduct contact tracing, and enforce quarantines. For instance, South Korea's epidemic-response statute enables authorities to collect mobile phone data from telecoms to reconstruct victims' recent whereabouts, then contact-trace others who may have come into contact with them; use of this data statutorily is limited to conducting activities related to combatting the spread of infectious diseases. In Hong Kong, following reports the government was considering using social media data to track potential COVID-19 carriers, the Hong Kong Privacy Commissioner issued a

statement that "there are sufficient legal and justifiable bases … on which the government may collect and use information obtainable offline or online … with a view to tracking potential COVID-19 carriers." Further, although difficult to verify through official sources, it has been broadly reported that China used telecommunications companies to track and contact people who had traveled through Hubei province during the early days of the virus, allowing Chinese authorities to re-create the steps of virus carriers and people that they may have encountered and issue warnings.

c. **Israel's Approach**: Israel's approach has garnered attention for its uniqueness. Benjamin Netanyahu's government issued emergency regulations to authorize the Shin Bet (Israel's internal security service) to use identifiable cellphone location data from customers in Israel and the West Bank to determine whether individuals have come into contact with COVID-positive individuals. Israel's legislation garnered significant criticism, and Israel's Supreme Court issued a temporary injunction against the new legislation several days after it passed, requiring Israel's Parliament to form an oversight committee before Shin Bet could use its new tracking powers.

d. **Canada's Approach:** Canada is reportedly declining to use any surveillance tools to track the virus at this point. Canada's Federal Public Safety Minister recently confirmed in a statement to the press that the government will "do everything in our power" to preserve civil liberties and personal privacy: "the law is still the law . . . and the highest law in the land is the Charter of Rights and Freedoms, which our government will always uphold." Currently, we have not been able to identify any publication that indicates the federal government has asked Canada's health or other agencies to obtain location or other mobile device data about the public.

3. COVID-19 Mobile Apps – Coming Soon from a Government Near You

In addition to the data-sharing measures outlined above, many national, state, and local governments have begun to develop mobile apps that help governments address various aspects of COVID-19.

a. Contact-Tracing Apps with a Privacy Focus

Potentially of significant interest for U.S. policymakers and companies is a class of mobile apps that have been developed to enable individual-level "containment" measures – such as contact-tracing and quarantine enforcement – on a voluntary and potentially privacy-preserving basis. Given recent expressions by U.S. public health experts on the importance of contact tracing and quarantining for long-term COVID-19 containment, apps designed to enable such measures in a privacy-preserving manner could offer significant support to COVID-19 prevention:

- Singapore is reported to have provided "proof of concept" for an app designed to enable contact tracing while preserving privacy, by publishing its app called "TraceTogether." Singapore's app works as follows: (a) when installed on a phone, the app generated a random encrypted identifier; (b) whenever the app comes into contact with another Bluetooth device that also has the app, it records that device's random ID – storing it locally for 21 days; (c) if a

user is later diagnosed COVID-19, her phone has a local repository of devices she was in contact with; so (d) all such "contacts" receive a notification on their phones informing them they are potentially exposed, and advising them to get tested.

- Starting in mid-March, German news reports indicated Germany's Heinrich Hertz Institute was working with a European team to develop a new privacy-preserving contact-tracing app. On April 1, "PEPP-PT" – which stands for "Pan-European Privacy-Preserving Proximity Tracing" – was launched. According to its site, PEPP-PT offers "standards, technology, and services to countries and developers" to enable "tracing of infection chains across national borders" under "a fully privacy-preserving approach." The head of Germany's federal privacy regulator tweeted that his office "provided tips and answered questions" to the team that developed PEPP-PT's technology (although it was not part of the initiative and did not issue formal approval). On April 9, France's Minister of Health and Secretary of State for Digital Affairs jointly announced in a press interview that France was developing a contact-tracing mobile app. In this interview, the Minister for Digital Affairs stated that app development is being led by task force headed by France's Inira research institute (which states it is a founding member of the PEPP-PT initiative), and relies on technology developed by "a European project led by Germany, France, and Switzerland" – suggesting France's app will use PEPP-PT technology.

- Furthermore, in the UK, Oxford researchers are working on a contact tracing app, based on research they have published in the journal Science. The researchers state the app will not track movements, but will instead "log a memory of all the app users with whom [a user has] come into close proximity over the last few days;" if any user becomes infected, all such contacts "are alerted instantly and anonymously, and advised to go home and self-isolate." App users can also permit the app to collect additional data to "identify trends," potentially indicating an analytics function.

- Additionally, as stated above, the European Commission announced it intends to work with Member States to publish a "pan-European approach" for COVID-19 mobile apps by April 15. European regulators have already tweeted that there will be a need for differences between Singapore's "TraceTogether" and European contact tracing apps. The intended involvement of the European Data Protection Board and European Data Protection Supervisor in the Commission's development of a pan-European app approach should ensure privacy regulators can represent privacy interests in this process.

b. Further Mobile Apps in Development Around the World

Apart from the above contact-tracing apps, governmental COVID-19 apps in other jurisdictions address a wide variety of use cases, and vary significantly in the degree of invasiveness and/or privacy protection they offer. These governmental apps are far from uniform and are designed to reflect local policy priorities; there is no one set of common functionalities to create a COVID-19 app. Apps have

been published by, *inter alia*, Argentina, Brazil, Colombia, Ecuador, Israel, Poland, Uruguay, Vietnam, and Indian states (e.g. Punjab):

- The Spanish Region of Catalonia was one of the first governments to offer a COVID-19 app, named "Stop Covid-19 Cat." The aim of the app is to enable self-diagnosis and avoid overuse of hospital facilities. Users who download the app take a COVID diagnostic test by inputting their symptoms, including their temperature, along with their ID number from their health insurance card (which can link to additional medical records). The app then provides heath recommendations to the user, and if an individual appears to be in a high-risk condition, medical personnel can contact them for treatment. The app also permits marking and statistical tracking of individuals suspected of carrying the virus for Catalan health agencies.

- In contrast, Poland's "Home Quarantine" app ("Kwarantanna domowa") helps Polish authorities monitor individuals who have been ordered to quarantine at home. Individuals under quarantine download the app, enable location tracking, and upload geotagged selfies at periodic intervals to confirm their presence within their home. Failure to upload the selfies or perform other actions prompted by the app can result in an automated alert being sent to Polish authorities. The app also enables quarantined individuals to make requests for in-home supplies (such as groceries) to Polish social services.

c. COVID-19 Mobile Apps in the United States

Within the U.S., mobile apps are beginning to play a role in COVID-19 efforts. The U.S. now has COVID-19 self-screening apps, as well as governmentally-issued contact-tracing apps:

- On March 27, the CDC, the White House Coronavirus Task Force, and Apple announced they have partnered to release a COVID-19 mobile app and website called "Apple COVID-19." The app contains a COVID-19 self-screening tool that "guides Americans through a series of questions about their health and exposure to determine if they should seek care for COVID-19 symptoms." The app then provides CDC recommendations based on the screen results, and information about when to contact a medical provider.

- MIT's Media Lab announced it has created a mobile app called "SafePaths", which also endeavors to offer "privacy-by-design contact tracing." Stanford University also announced it is developing a contact-tracing app called "COVID Watch," which it states will be designed to provide "privacy-preserving, decentralized Bluetooth contact tracing." It is currently unclear if any governmental apps have integrated SafePaths or COVID Watch technology.

- On April 8, the State of North Dakota announced it was launching "Care19," a contact-tracing app. Care19 users can enable the app to collect their location information to aid North Dakota's Department of Health in contact tracing efforts. The app description indicates users' location information will be collected over time, but only shared with the North Dakota Department "if [the user] consents upon testing positive for COVID-19." The app's Privacy Policy indicates that

location data collection will occur periodically irrespective of whether the app is running, and may be used to help calculate a "personal risk score" for users which can be shared – on an aggregated basis – with North Dakota officials.

- Lastly, as noted above, Apple and Google announced a partnership to create a broad "Bluetooth-based contact tracing platform." One stated aim of this platform is to "enable interaction with a broader ecosystem of apps and government health authorities," and it may thus lead to broader COVID-related app creation.

* * * * *

COVID-19 may be an opportunity for telecommunications and technology companies to work towards a uniform privacy-protective protocol that could be used in response to government requests for mobile phone data. Particularly with the CDC moving towards data-driven solutions, technology and telecommunications companies should work now to assess if and how they may be able to offer significant help in the fight against COVID-19.

Alston & Bird has extensive experience in responding to governmental data requests, working through protocols for such responses, and coordinating such efforts with companies' overall compliance efforts.

For further information, contact Jim Harvey, David Keating, Kim Peretti, Wim Nauwelaerts, Amy Mushahwar, Kathleen Benway, Jon Knight, or Daniel Felz.