Location, Location, Location: What Will Your Personal Data Reveal Besides Whether or Not You #StayHome?

03/27/2020

As more and more Americans are learning the ins and outs of Zoom, receiving baptisms by fire in the world of homeschooling or simply catching the latest episode of "Tiger King," we are now on more screens than ever. Inevitably, more screen time leads to more social media and online surfing.

Last week, *The Washington Post* reported the U.S. Government is in discussions with tech companies, including Amazon, Apple, Facebook and Google among others, regarding the use of anonymized and aggregated geolocation data to track social distancing compliance in response to the COVID-19 coronavirus (in addition to assisting epidemiologists in spotting trends).[1] Similarly, Italian companies, LogoGrab and Ghost Data, collaborated to harvest images and video of 552,000 profiles and public Instagram stories from March 11-18, 2020. This data was anonymized and processed to identify the level and types of violations during Italy's initial period of lockdown.[2] On March 24, 2020, Uncast launched a "Social Distancing Scoreboard" that evaluates behavior using GPS location data.[3]

Although sources claim information is shared on the aggregated level and that the government is not looking to build a central database, consideration of these potential new uses makes it as good a time as any for a reminder of what accounts and devices collect location information.

Facebook and Instagram: These platforms collect content users provide when the platforms are in use, such as location of a photo or the date a file is created, and contact information if a user uploads, syncs or imports that information from a device. [4]

Google: Google tracks users' location data when its services are used, meaning each time a user searches on Google, watches a YouTube video or uses Google Maps.[5]

Amazon: By searching, shopping, downloading or providing account information users also may supply Amazon with location information.[6]

TikTok: TikTok automatically collects location information based on your SIM card or IP address and with users' permission, GPS data.[7]

Zoom: In addition to collecting information about its users' devices, Zoom also collects Facebook profile information when Facebook is used to log in to use Zoom's offerings.[8]

Apple: Although location services can still be completely disabled in iPhone settings, Krebs on Security reported the iPhone 11 Pro periodically collects location data even in the disabled setting by periodically sending geo-tagged locations of nearby WiFi hotspots and cell towers in an anonymous and encrypted form to Apple.[9]

From the list above alone, there are plenty of sources available to tap for this information. The World Health Organization has stated more technological measures are needed for tracking the coronavirus outbreak, essentially asking world leaders to prioritize human lives over privacy. Despite many countries, such as the U.S. and EU, having stringent privacy laws, governments all over the world are either already relying on mobile carrier data to track social distancing and shelter-in-place declarations or are considering it.

But what are the lasting effects of this hopefully short-term intended use? Tracking can carry privacy risks because location data can reveal a lot of sensitive information about how we live. Currently, discussions focus on aggregated data but should the pandemic worsen, requests for data could become more specific. Similarly, there are concerns that this information could be further shared or sold to third party aggregators for further profit. The United States currently does not have a centralized approach to data privacy issues, so any changes in data protection will have to navigate state and sector-specific regulations. Additionally, American companies have a long history of credibility issues with the U.S. public when it comes to controversies surrounding personal data. We have already seen big changes in the privacy legislative landscape in the form of the General Data Protection Regulation, the California Consumer Privacy Act and the New York Department of Finance Cybersecurity Regulation in response to the misuse of personal data by private companies. Abuse of these potential new uses of location data may inadvertently end the use of location data for marketing purposes in the long run.

---

[1] https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/

[2] https://blog.logograb.com/covid19-visual-ai-analysis-lockdown-violation-italy/

[3] https://www.unacast.com/covid19/social-distancing-scoreboard

[4] https://www.facebook.com/policy.php

[5] https://safety.google/privacy/data/

[6] https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_87C837F9CCD84769B4AE2BEB14AF4F01

[7] https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-us

[8] https://zoom.us/privacy

[9] https://krebsonsecurity.com/2019/12/the-iphone-11-pros-location-data-puzzler/