LOCATION TRACKING: WHERE TO DRAW THE LINE

Christian King

Abstract

The widespread adoption of cellphones, and more recently smartphones, has opened up the door for companies, such as Verizon, AT&T, Google, etc. to remotely track an individual's location. How does location tracking benefit the user experience? What sort of government regulations surround the recording of location tracking data? Can users trust that companies will respect their desire for privacy and confidentially handle such data? Currently, there are few legal regulations governing the collection and processing of location data, allowing for its potential misuse by government entities and marketers.

Keywords: Location data, geofencing, location tracking, ethical, data privacy

Table of Contents

Introduction

With the widespread usage of smartphones and the rapidly developing cellular data infrastructure, smartphones and other mobile electronics are almost always connected to the internet and cell towers. Often, smartphones track their user's precise location and apps use this locational information for their core functionality. Location data is currently being used in many different ways: mobile ads, social networks, transit apps like Uber and Lyft, as well as in commercial analytics systems, and business intelligence software. The rapidly progressing technology in the smartphone industry continuously adds more and more functionalities that rely on location data. The sheer amount of collected and processed location data allows for the creation of detailed maps of user behavior. As this happens almost automatically while users go about their day-to-day activities, they are often unaware that they are tracked, not knowing how much information they share or with which parties. With the ability to track an individual's movements at an unprecedented level of detail, government regulations should be put in place for companies that collect location data. It must be ensured that these companies collect this location data without violating users' expectations of privacy.

Legal Precedents

The greatest ethical dilemma surrounding location tracking data is the potential for it to be used within a court of law. The practice of collecting user location data is still in an early stage, and there are many legal grey areas related to privacy and federal legislation surrounding the matter has yet to be enacted. While law enforcement is required to obtain a search warrant in order to access this data, there is no law requiring Google Maps or Apple Maps to keep user GPS data private. In 2018, the Supreme Court agreed to hear the case, Carpenter v. United States, in which the dispute was whether evidence obtained through GPS tracking is admissible in court. The court determined that government entities must obtain a warrant to access cellphone location information (Carpenter v. U.S, 2018). Without a warrant, it can only be used against a suspect at the judge's discretion after being found not to be prejudicial to the defendant's rights. This case demonstrated that the American judicial system is taking the rapid advancement of technology seriously.

There have been some strides in legislation to protect users' privacy rights. The Electronic Communications Privacy Act, enacted in 1986, was designed to protect electronic data left on-site or at another person's home, though it is woefully out of date and does not take into account the way people use their smartphones and other mobile devices. This Act has been amended several times since its inception, but lawmakers have yet to address the legal ramifications of pulling location data from smartphones and other internet-enabled devices (Gross, 2010). Additionally, in November 2017 the California Consumer Privacy Act (CCPA) was signed into law. The CCPA requires companies to get written consent from users before collecting their personal, non-public location data. The law also states that companies must disclose how this data is used and how long it will be stored. The bill requires a person to receive

notice about practices that are intended to collect (GPS) information, provides an exception for emergency situations, and protects the right of California consumers to control the use of their personal information. The bill explicitly states that California's legal protections apply to "any other data or information pertaining to a consumer's physical location, including any other personally identifiable location data" (State of California, 2017). Legislation, both at the state and federal level, is constantly evolving, as many privacy advocates argue that location data should be protected under the fourth amendment.

Corporate Monetization

Another ethical concern of location data tracking is its usage in marketing. Geofencing ads have become quite commonplace with modern technology and have in some ways completely changed the advertising industry. Geofencing is a tool that uses an app's GPS data to identify when it enters or leaves a particular geographic zone (Koyak, 2021). A company can then deliver ads specific to the location, or target their marketing based on the locations visited. Historically, companies have advertised their goods and services to the general public by employing a variety of mediums and forms of marketing, such as commercials, billboards, flyers, or ads run on television. The sheer volume of ways in which businesses can advertise in this modern era is astounding. Geofencing has made advertising very precise, as ads can be delivered only to people within a certain distance from a business's location. This has allowed for advertisers to reach users at the point of purchase with relevant ads, as well as provide new user generated content for businesses. It also allows for marketers to analyze customer data and their behavior in a way that wasn't previously possible.

While this technology is new and exciting, there are some ethical concerns arising from its widespread usage. For example, in 2015, a Massachusetts-based, digital advertising company was hired by a Christian pregnancy counseling and adoption agency (Allyn, 2018). The advertisers created a geofenced area which surrounded numerous methadone clinics and reproductive clinics (i.e., Planned Parenthood). Advertisements with messages such as "Pregnancy Help," "You Have Choices," and "You're Not Alone", were sent to the devices of users within the geofenced area. Once clicked, the user would be redirected to a webpage discussing abortion alternatives and offered counseling with a "pregnancy support specialist" (Commonwealth of Massachusetts, 2017). This showcases just one of the many ways in which geofence marketing can be used to prey on consumers. The geofenced abortion clinic marketing situation is an outright invasion of privacy; proper consent should be requested from the user prior to the initiation of geofencing. And furthermore, companies should work to be transparent about their practices and explain to the user which parties will have access to their location data. In addition to legislation, there are many companies that have voluntarily put forth privacy policies that outline their usage of user location data. For example, Google has its "Location History" feature in its settings menu, so that users can see what information they have shared with Google and its partners. Google also has a privacy center that allows users to manage their location data. Another example, Apple has a "Location Services" setting in which users can see what apps are using their location data and turn off access if they choose. These steps, which have been taken by several large companies, could be a step in the right direction towards empowering people in relation to their own privacy rights.

Benefits of Geofencing/Location Tracking Data

Alternatively, it could be argued that collecting this data may be for the greater good in multiple ways. For one, it greatly aids law enforcement in preventing and investigating crimes. In the case of Carpenter v. U.S., Timothy Carpenter had been responsible for a series of armed robberies in the Detroit area (Cornell Law School, n.d.). The cellphone location data was greatly beneficial in building a case against Carpenter. Location data can help to identify potential suspects, especially when there weren't any witnesses to a crime scene. The location data can place a suspect at the scene of the crime, allowing law enforcement to rule out innocent parties and focus their efforts on the guilty party. However, while it may be true that location data could be effective in stopping crime, this data should still be treated with confidentiality by the companies that record it and not simply handed out to any government officials on a whim. One such case of this data simply being handed out "on a whim" took place in Milwaukee, Wisconsin, in 2019. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) demanded Google hand over the location data of all devices within a 29,387 square meter area. Google obliged, handing over the location data of 1,494 identified devices (Brewster, 2019). Based on Google's actions, it's clear that there is very little regard for protecting this location data. Doing such a broad sweep of information seems completely unwarranted and, in this case, it could have jeopardized the privacy rights of hundreds of users. A line must be drawn that protects innocent users from being categorized as potential suspects in these Geofencing searches.

The location tracking data can also grant an improved experience for smartphone users. Apps such as Uber and Lyft are able to gather data on users' travel habits and the likelihood of them turning on the app for specific routes at certain times (Roman, 2016). In order to make

transportation more efficient, Uber created web-based interactive maps which show a key between locations that allow users to see how long it would take them to get from one place to another. This is a great experience for consumers and offers some degree of convenience in their day-to-day travels. Another benefit of location data is in the area of public health. For example, during the peak of the COVID-19 pandemic, Israel deployed a location data tracking system which would send out alerts if an individual had been in contact with a confirmed carrier (Altshuler & Hershkowitz, 2020). With this system, the movement of people could be mapped and used to predict where and when new cases would arise. So evidently, there are some positives that come along with tracking user location data. However, privacy watchdog groups felt that Israel's COVID-19 tracking system was overly invasive. In 2021, the Supreme Court of Israel ordered that this surveillance program be shut down, citing concerns about the program being an invasion of privacy (Estrin, 2021). With this situation, it's evident that while the Israeli government may have been trying to go about keeping its citizenry healthy and safe, it also crossed an ethical line. The simplest solution to this would to have created a voluntary, opt-in program that requests a user's consent before tracking their location and sending them alerts.

Conclusion

The debate on location privacy rights comes down to whether or not the collection of this information can be ethically justified. Individuals must ask themselves which parties have access to their location data and what can those parties do with it. Evidently, the collection of location data could allow businesses and government entities access to highly accurate and potentially sensitive location-identifying data, which they've historically never had the ability to monitor. As technology continues to evolve, so too should the legislative and judicial precedents regarding location data. There are many societal benefits that this technology can offer us, when used

ethically. Tracking location data should not be completely forgone because of its potential to be used in a corrupt manner. To ensure that this data is kept secure and only used with the explicit consent of a user, comprehensive legislative policies must be put in place to draw the line and demonstrate the standard to which this privacy data should be treated. Additionally, it should be the onus of companies collecting this data to inform the user about how they are handling their location data and whom they may share the location data with.

References

Allyn, B. (2018, May 25). *Digital Ambulance Chasers? Law Firms Send Ads To Patients' Phones Inside ERs*. NPR. Retrieved April 13, 2022, from https://www.npr.org/sections/health-shots/2018/05/25/613127311/digital-ambulancechasers-law-firms-send-ads-to-patients-phones-inside-ers

Altshuler, T. S., & Hershkowitz, R. A. (2020, July 6). *How Israel's COVID-19 mass surveillance operation works*. Brookings. Retrieved April 13, 2022, from https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillanceoperation-works/

Brewster, T. (2019, December 12). *Google Hands Feds 1,500 Phone Locations In Unprecedented 'Geofence' Search*. Forbes. Retrieved April 13, 2022, from https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leadsto-arsonist-smartphones-in-unprecedented-geofence-search/?sh=26c790c127dc

California Consumer Privacy Act (CCPA). (2022, March 28). State of California - Department of Justice - Office of the Attorney General. Retrieved April 13, 2022, from https://www.oag.ca.gov/privacy/ccpa

Commonwealth of Massachusetts. (2017, April 4). *AG Reaches Settlement with Advertising*

Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities. Mass.Gov. Retrieved April 13, 2022, from https://www.mass.gov/news/ag-reachessettlement-with-advertising-company-prohibiting-geofencing-around-massachusettshealthcare-facilities

Estrin, D. (2021, March 1). *Israel's Supreme Court Ends Spy Agency Cellphone Tracking Of COVID-19 Infections*. NPR. Retrieved April 13, 2022, from https://www.npr.org/sections/coronavirus-live-updates/2021/03/01/972560038/israelssupreme-court-ends-spy-agency-cellphone-tracking-of-covid-19-infections

Gross, G. (2010, September 22). *Senators Push for Update to Electronic Privacy Law*. PCWorld. Retrieved April 13, 2022, from https://www.pcworld.com/article/503355/article-2824.html

Horn, M., & Wouters, C. (n.d.). *Carpenter v. United States*. Cornell Law School. Retrieved April 13, 2022, from https://www.law.cornell.edu/supct/cert/16-402

Koyak, B. (2021, August 30). *Digital Marketing: Geo-fencing*. Laurus College. Retrieved April 14, 2022, from https://lauruscollege.edu/digital-marketing-geo-fencing/

Roman, L. (2016, December 1). *Uber Now Tracks Passengers' Locations Even After They're Dropped Off*. NPR. Retrieved April 13, 2022, from https://www.npr.org/sections/alltechconsidered/2016/12/01/503985473/uber-now-trackspassengers-locations-even-after-theyre-dropped-off