Lexi Weingardt

Professor Johnson

CMSI 401

10/7/20

Assignment #1

The article "A Closer Look at Location Data: Privacy and Pandemics" addresses the impact of the pandemic on location technology and the ethical concerns involved. The author, Stacey Gray, begins by discussing the increased interest recently in location data and how countries across the world are using this information in an attempt to better contain the virus. Gray provides an example of this in South Korea, where they have "created a publicly available map of location data from individuals who have tested positive". Gray goes on to describe precise location data and how it is being used in this context. Precise location data involves "information about how devices and people move through spaces over time". Interest in gaining people's precise location data has piqued due to the pandemic, but it comes with a variety of privacy concerns, which I will discuss later on in my summary. Gray also discusses who has access to this location data and how it is collected. Location data can be held by a wide range of entities including mobile phone carriers, operating systems, apps, location analytics providers. Your location data can be collected using GPS, cell towers, Wi-Fi networks, etcetera. This allows for many people to collect your data and use it in a variety of different ways, which ultimately leads to concerns about privacy. Precise location data in particular is very sensitive and there are a lot of laws in place in order to protect users. Oftentimes, precise location data is deemed acceptable to use given that it is anonymized or aggregated, but this is actually very difficult to do and still in some cases does not fully protect users' privacy. In addition, the author addresses issues of bias when using location data, as well as the possibility of the data being used for purposes other than collecting pandemic data.

The situation described above is crucial when you are designing or developing software. As many events of the past will show you - an example being the global surveillance after 9/11 - technology can be very dangerous when used incorrectly or without regard to any ethical standards. Cybersecurity has become even more important in recent years, and is now one of the biggest concerns when developing new technologies. As software developers, specifically, it is largely in our hands to make sure that our projects and technologies do not infringe on users' privacy in a potentially dangerous or harmful way. We can do this by making sure that we follow regulations that have been set for us by our state (for example California has the California Consumer Privacy Act). We can also make sure that we are using trustworthy security models and that we have people on our team who are concerned primarily with security. It is very important to ensure that all these factors are in place, because a failure in security can have a huge impact on the technology itself and the people who use it.

In addition to location information, another important privacy concern in recent years has been personal information. With the development of social media and other platforms, this is more crucial than ever, as can be seen in the loss of consumer confidence after Facebook's data scandal. The scandal involved the data leak of millions of Facebook users' personal information without consent. This then resulted in an online movement to get rid of Facebook. If users do not feel a sense of trust when using your product, it is much less likely they are going to continue to use it. Software developers have a huge responsibility to create software that will develop and maintain this trust. This can include having privacy policy agreements which hold companies to certain standards upon collecting user data. Having a policy which developers and the business or company using the technology agree upon is a way that developers can directly impact and protect users' privacy. Another way developers can protect user data is letting the users themselves have control over the data they share and don't share through the use of preferences. This can be very impactful and I think it is one of the best ways to protect user privacy. I like that it gives control back to the user and lets them have power over what they choose to share. This is more and more prevalent in modern technologies, particularly applications, such as social media apps, which have the ability to collect and display a lot of user information, including their location. Ultimately, these are some simple ways which allow developers to have a huge impact on user privacy and give users a sense of trust in a technology or application.

As we have seen above, it is also very important for developers to maintain that sense of trust by preventing data leaks of sensitive information when at all possible. First of all, it is important to treat sensitive data differently and to be intentional about how and what data can be accessed. On the backend, you should not be using the data collected on any other environments, as that could result in data leaks. Other ways to increase security on the backend include encrypting backups and restricting access. Developers should be continually making sure that the data is only being accessed by those who have permissions to do so. Another easy way to accomplish this that I have seen is by updating your libraries and your software. Although this is something that developers should be doing already for several reasons, it is also a great way to keep your technology secure and protect users' privacy. One of the last ways I've found that developers can increase security is by simply not collecting more data from the user than needed. Ultimately, I can apply these methods of protecting users' privacy when I'm developing software by being more conscious about the data I am getting from the user and who has access to said data. All of the strategies mentioned above are great ways to ensure that users' privacy remains protected, which is crucial in the development of technologies today.

Bibliography:

Daan. "Privacy and Data Protection." *Medium*, Better Programming, 30 Sept. 2019, medium.com/better-programming/privacy-and-data-protection-c4f38678c639.

David Oragui / 4 February 2019. "David Oragui." *The Manifest - Small Business News, Data, and How-To Guides*, themanifest.com/mobile-apps/4-reasons-your-app-needs-privacy-policy.

"Future of Privacy Forum." *Future of Privacy Forum ICal*, 25 Mar. 2020, fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/?mkt_tok=eyJpIjoiWXpCbFpHUTJNVGRsTVdSaiIsInQiOiJLSjVjSFwvMnI0TVI4bExcLzJ5aGJ0VHd3VytEMTErbStacUdRdTZRZitQTXVuT2lkUTVRSmZEa2xZZEJLN3FhNHlncjFxTjFFWWJhdEs1alpjUkdnazFaRmRLVkFYU2JPVForWm1mbnFUcENJWmRWaUEzZ1EyK1wvb01MSXo4cno0WCJ9.