Zachary Hightower Essay 1: The Right to Privacy

Privacy is a right in the United States. How far that can extend and how it should be handled is not so black and white. Web privacy often changes priority with the perspective that someone views it from. A user often views it with ambivalence or very protectively. From the perspective of large advertising agencies or data scientists, the flow of data to them is important. Once they have an influx of user data, they want to keep it and grow it if possible. These people benefit from having privacy for users very loose. However privacy of their datasets is a priority. These are the large forces that drive most legislation involving privacy on the internet. This essay examines the depth of these interactions. We also look into how the available tools can be used to make better decisions and how decisions regarding privacy should be made.

Google Maps, and other GPS directions applications require a good deal of privacy to be given up in order to access their features. It provides us with the ability to know the shortest path to where we want to go, incredibly accurate estimated time of arrival, and even updates in real time on traffic changes. All of this is made possible by giving up information about where we are and where we are going. This is something most people are not happy to tell a complete stranger. However, as the company reports, Google Maps has more than a billion users. That means that more than thirteen percent of the humans on earth are being voluntarily tracked by Google. People regularly make the choice to give up their location information. Users may not know the full breadth of privacy they are giving up, though. Benjamin Baron and Micro Musolesi studied the habits of users and created profiles that, from location data, allowed them to predict many other traits of their users (Baron & Musolesi, 2020). Giving up data does reap a significant reward, but it is often difficult to understand how much data is actually being given up. Users should have all the information available to them when they make decisions about whether or not to give away parts of their right to privacy.

There is some push back against constant tracking that occurs on the web. It is more common now to see sites that actually inform the user about cookies give the ability to opt out of unnecessary

ones. Contrary to popular conception, cookies can be used constructively. A helpful example of cookie use is provided in, “Taking the Byte out of Cookies”, where a cookie is proposed as an alternative to storing user information in a central database. In this example, the cookie allows a user to take their information with them when they leave the site. This is a massive boon to the user’s security, since it means that if the site’s database is compromised, whatever information has been stored in the cookie can’t be accessed by the bad actors (Lin & Loui, 1998). However, as can be inferred from the proliferation of anti-tracking extensions on websites, this is often not the aim. Cookies can also be used to track user preferences and harvest data that the user may have no idea is being given up. It is also sometimes that the company wants to store the user’s data in their central database, so it can be used and sold.

It is important to consider more oversight and stricter standards for American privacy on the web. Data can be anonymized. Data can be encrypted. Data can be split up into different portions so that no one access point being breached turns into a massive compromise. These methods, and the methods by which combination of data can lead to privacy compromise beyond what a user is usually told can be found in Protection of Big Data Privacy (Mehmood, Abid, et al., 2016). Knowing all this, we cannot expect to have full privacy on the web. However, we can push for greater security and more intelligent construction that allows us to keep the features we need, while minimizing the risk personal data leakage.

References

Baron, Benjamin, and Mirco Musolesi. “Where you go matters.” *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 4, no. 4, 17 Dec. 2020, pp. 1–32, https://doi.org/10.1145/3432699.

Lin, Daniel, and Michael C. Loui. “Taking the byte out of Cookies.” *ACM SIGCAS Computers and Society*, vol. 28, no. 2, June 1998, pp. 39–51, https://doi.org/10.1145/276758.276775.

Mehmood, Abid, et al. “Protection of Big Data Privacy.” *IEEE Access*, vol. 4, 2016, pp. 1821–1834, https://doi.org/10.1109/access.2016.2558446.