Assignment: Ethical Case Study Analysis

Michael P. Currier

University of South Florida, School of Information

LIS4934: Information Science Senior Capstone

Dr. Richard Austin

October 9th, 2023

Assignment: Ethical Case Study Analysis

The Internet of Things (IoT) is a far-reaching term that is used to describe the network of any electronic device that has access to the internet. Internet access is becoming the norm for more than just traditional devices like smartphones or computers and is now a critical feature of objects like watches, refrigerators, and cars to name a few examples. These devices also create a massive amount of data generated by the device's user(s), allowing for detailed user data profiles to be stored and sold. Such an abundance of data-collecting devices and the potentially sensitive data they extract can, has, and will continue to create privacy concerns for the people behind the screens. Paired with the rapid development of more sophisticated machine learning algorithms, the organizations that collect, store, and sell user data have an inherent advantage over their competitors who have not had the same amount of time to build such detailed data profiles. Not only will this affect basic user privacy but will stifle competition in the marketplace and give birth to data-driven monopolies. This paper intends to examine those consequences and suggest steps to be taken to alleviate said consequences.

As the IoT finds itself spanning into more components of daily life, the software that develops user profiles will become better tailored to the individual user. For example, the music playing from an IoT device may change depending on data collected from a separate IoT device to better suit the setting. Such advanced algorithms are potentially even "able to predict what you want before you even know you want it" (Strickland, 2013). Without looking deeper into the implications or consequences of such technology, this may appear to be nothing more than an opportunity for well-targeted marketing. When looking at the implications, the timeline must be considered. Traditionally, transactions for things like household appliances are one-dimensional; the exchange is made, and the transaction is over. More complexity is added when dealing with IoT devices which continuously collect valuable data from that customer, creating value from the

consumer far past the initial transaction. Over a longer span of time, the data generated about that consumer often becomes more valuable than the device that collects it.

This creates a contradiction with the argument made in Karsten's article which claims that the IoT can "democratize innovation" (2016). The article argues that the pervasiveness of IoT devices will give average consumers more sway in innovative solutions and stop any one group from obtaining too much decision-making power in the marketplace. This argument is weightless because that data is stored and owned by groups that already have the capacity to roll out IoT devices on a large scale. The opinions and criticisms held by the public on their smart-fridge have no chance of introducing external innovation to the marketplace if the only organizations that have access to it are the ones who made the smart-fridge. In fact, this would only further monopolize that organization's market control by giving them more data to use versus new competitors.

When addressing this issue, one reasonable approach is to create more transparent user data policies that state specifically what data is being stored and where it is being shared. A user's consent to share their data may be subject to change based on where that data is being shared, meaning users should be informed on all the possible uses of their data with as much detail as is known by the seller. An important distinction to make for legislators is that personal information gathered from users is not the data-collectors product to sell without consent; it belongs to the user. With this train of thought, it would not be unreasonable to consider creating regulations that define a user's data as their own protected asset rather than a sellable commodity for the data-collector.

It is important to think about this topic from a critical yet realistic perspective. While data collected from the IoT is a powerful tool with the potential to create a smarter cyberspace, it also gives the collectors of that data an inherent advantage over their competitors which can create

unfair market conditions. Further, the data being collected and sold by such collectors is being taken from users who often have little understanding of how their personal data is being handled. It is important for regulators to make the distinction that a user's data is their asset to manage, not the collector's. At the very least, users should have as much knowledge of what will be done with their data as those who are collecting/selling it.

References

Karsten, J. (2016, July 29). *Alternative perspectives on the Internet of Things.* Brookings. https://www.brookings.edu/articles/alternative-perspectives-on-the-internet-of-things/

Singer, R. W. et al. (2015). Wearables: The well-dressed privacy policy. *Intellectual Property & Technology Law Journal, 27*(7). https://link.gale.com/apps/doc/A420929651/AONE?u=tamp44898&sid=bookmark-AONE&xid=74b7983c

Strickland, J., [Fw:Thinking]. (2013, March 1). *What is the internet of things?* [Video]. YouTube. https://www.youtube.com/watch?v=LVlT4sX6uVs