Yusra Ashar

CST 300 Writing Lab

9 October 2024

LoT Data Privacy: Balancing Innovation and Privacy

The Internet of Things (IoT), a network of interconnected devices that can communicate and exchange data, has transformed the interaction between persons and technology. The stem of the technologies IoT allows interconnections of everyday home appliances like home assistants, wearables, and intelligent locking systems, where the devices capture, exchange, and process significant volumes of personal information to increase their usefulness and effect. However, such advances come at a cost; increased usage of these devices also raises the issues of data privacy and security as more users' data is being collected by these devices even though they may not have expressly approved it.

The less concern for privacy and increased use of IoT has become unethical because of the nature of information such IoT gadgets will gather, such as discreet locations, biometrics, and favorite things by the person. How this information is governed by different organizations in the world has become one of the sources of the ire of modern-day people. The trends seem to imply that as more people connect to the internet, which gives rise to the number of connected devices, the level of intensity toward protecting privacy and securing sensitive information will increase (Weber, 2010). Over the past few months, numerous high-profile data leaks and invasions of privacy related to IoT gadgets evinced the threats posed by not protecting privatized information. This creates a conflict and tension between two actors, one for IoT manufacturers who voice the need for data to advance innovation and consumers who are more privacy-oriented and want regulation these days.

Solving problems in everyday life and making life more comfortable were the primary causes for IoT's inception and development. As a result, providing real-time information and services to users, as well as products such as smart home appliances and health trackers, have become standard practices. Nonetheless, as IoT technology has matured, the amount and extent of the data collection process has grown, too (Schneier, 2018). However, ethical controversies concerning innovation versus privacy are pretty standard. Both sides have reasonable arguments.

Stakeholder Analysis

Stakeholder 1: IoT Device Manufacturers

Companies producing IoT devices, such as Amazon, Google, and Apple, are more concerned with innovating new products and enhancing user experience. These companies, referred to as 'IoT Device Manufacturers', say that data is critical in constructively determining how people will use IoT devices and the services that should be provided. The provision and processing of user data help match the manufacturing process with the needs of the consumers more innovatively (Bandyopadhyay & Sen, 2011). In the specific scenario, for instance, a smart home assistant observes how people use it over time and adapts accordingly, making it only better at responding and performing more duties. The manufacturer's position is that without collecting data, 'progress' cannot occur, and in the development of IoT devices, their advance will simply drift.

The manufacturers consider the high level of attention to the development of technological processes, improving the efficiency of the company and the satisfaction of consumers. They think collecting this kind of information means creating better and more innovative devices and services that will benefit society overall. From their perspective, the upsides of data collection,

such as enhancement of usability and improvement of device functionality, exceed the downsides, which concern the invasion of privacy (Alaba et al., 2017). Additionally, they claim that the data collected is 'given' by the users when using the IoT tools and accept their terms and conditions.

IoT creators argue that data harvesting is for the common good because it allows users to improve their offerings. Therefore, the majority of users will be happy. They argue that through information collection, they can enhance user experience, which in turn enhances their performance and fosters new developments. This is why privacy concerns relating to extensive data collection are usually surmountable: Supporters think such an invasion is for the greater good, as others will benefit from it (Herold, 2020).

Stakeholder 2: Consumers and Privacy Advocates

On the other hand, consumers and privacy advocates maintain that respect for personal privacy and autonomy comes first. They hold that IoT companies should not seek and obtain regular citizens' personal information without their explicit informed consent. They also argue that consumers need to know how their personal information is being gathered, processed, and applied, and more importantly, they have to be given the power to manage this information. This emphasis on the importance of consumer consent in data collection fosters a sense of empowerment and control among the audience.

Consumers and privacy advocates highly value privacy in terms of personal responsibility, equity, and privacy. They claim that the present practices of data collection involving the IoT encroach on the privacy of the users as a majority of them need to be made aware of to what degree their information continues to be amassed and reused. These stakeholders expect firms to

assist them by clarifying their data collection policies and supporting them to ensure data is not collected illegally without users' consent. They opine that clients are entitled to agree or refuse to join in data sharing, and companies should not only be committed to offering products but also ensure adequate security of personal information (Ziegeldorf et al., 2018).

It has been argued by privacy activists that IoT companies take advantage of users' ignorance regarding data collection when infringing on their privacy. They claim that no company should be at liberty to collect any data from its users unless that data is willingly given to them and that individuals should be in control of the data relating to them or their information. This viewpoint is based on deontological moralism, prioritizing respecting peoples' rights and complying with obligations. Privacy advocates also claim that companies should tend to privacy more than profit and innovation (Weber, 2010).

Argument Question

The issue of whether IoT companies should be allowed to mine and store personal data without the knowledge and approval of users is heated as it raises the trade-off between privacy and the desire for innovation. Their position is that data collection helps develop better functional products, bring on better user experiences, and advance technology. They argue that the legal provision has been complied with by saying that acceptable data may be collected and used where consent is given implicitly at the agreement of terms and codes of conduct. On the other hand, privacy advocates argue that freedom of an individual or person's fundamental rights can only be exercised satisfactorily where individual informed consent is obtained in using individual personal data. On that account, they claim, however, that such practices by organizations that direct opt-in and opt-out methods of data collection and usage should not be

the case. Allowing companies to gather data without informed and explicit consent from their clients poses great ethical dilemmas, such as possible misuse and data breaches, as well as diminishing the relationship between end users and companies. Hence, the conflict arises from whether the advancement of technology outweighs the violation of core human rights to privacy.

Stakeholder 1: IoT Device Manufacturers

The position taken by IoT device manufacturers agrees with utilitarianism, an ethical theory pioneered by Jeremy Bentham and John Stuart Mill. According to the basic tenet of utilitarianism, the consequences of an act determine whether it is right or wrong, and assuming rightness, how much benefit can be derived – in other words, the objective is to provide the most significant advantage to the largest number of people. Utilitarianism allows a particular course of action, irrespective of whether it is against the interest of the few people, as long as it aids the well-being of the many. On the other hand, IoT manufacturers consider it quite reasonable to justify the threat to privacy for product and service enhancement, which will likely be of better utility for most users.

According to the utilitarianism doctrine of ethics, IoT manufacturers state that extracting personal information from users is for their own good. It fosters technological achievements and provides better services to numerous consumers. The payments tend to increase gradually with an increment of data collected; such companies are in a position to offer customized services, make intelligent machines, and achieve productive efficiency. This information collection tends to create a cycle of innovations that advances society. There are views against the data collection that the individual's privacy is infringed upon. However, the producers say that these experiences

and services that depend on data collection are more advantageous than detrimental. Thus, manufacturers consider this perspective an ethical and utilitarian notion.

In the eyes of IoT manufacturers, pursuing data in a ”sneaky” way is justified, given that society as a whole reaps the maximum benefits. This data collection enables the personalization of services and the enhancement of product development in line with other businesses in a fast-integrating technological environment. However, they assert that reasonable innovation will always come to a standstill if the manufacturers are not allowed to gather data, and the users will forfeit the benefits of advanced technology. The little privacy that some people may lack has negative implications. However, for most users, these are outweighed by enhanced products and services, and this is the ethical action taken under utilitarianism.

IoT manufacturers stand to gain significant advantages if they continue collecting personal data and storing it without the user's permission. More advanced devices would be available, individualized services would be rendered, and market competition would be retained. This would lead to a higher level of satisfaction by consumers and the growth of the business. However, suppose the mentioned manufacturers have to inform and get consent from the consumer. In that case, they will be met with difficulties in acquiring the same amount of data, which will, in turn, hinder innovation, and alternative services will be offered. This will severely puncture their efforts to enhance and improve the quality of their services, hence risking losing consumers’ trust and market share.

Stakeholder 2: Consumers and Privacy Advocates

The position adopted by consumers and privacy activists corresponds with deontological ethics, which, in general, is connected with Immanuel Kant. Instead, it would be none because

deontological ethics makes those who adhere to the ethical rules and the individual's rights irrespective of the results achieved. The principle of this approach is that a specific action, in itself, always involves something good or evil. It implies that there is an ethical approach companies must take where one's privacy and sovereignty as an individual must be observed. This is regarded as simply wrong; approval of data collection without permission, even for reasons that appear just, violates users' rights.

Deontology places responsibilities on consumers and privacy advocates concerning IoT companies. For such companies, protecting an individual's privacy is a moral obligation, and this obligation cannot be dismissed because of the advantages that can be gained from data collection. In the description, it appears that people have unalienable rights over their data, and there is no justification for infringement of this right for any possible benefit to society. People who defend privacy rights point out that people's prior express consent should always be gained, and this should include the collection of any data about individuals to avoid violating people's rights to make choices concerning their privacy. This ethical obligation to safeguard privacy concerns the argument of no data collection without consent.

From the perception of consumers and the advocates of privacy, the only permissible action from a moral standpoint is that IoT companies should seek the user's permission before collecting personal information. Such a course of action preserves the person's privacy and self-determination rights, which should never be compromised for ease or progress in technology. Deontological ethics, on the other hand, holds that certain rights, such as privacy, are instrumental and cannot be violated for the greater good of society. Against this background, insisting on explicit consent to change the inner family regarding IoT seems to be the adequate and responsible way out.

Regarding the evolving digital landscape, privacy protection is envisaged to be enhanced as consumers and privacy advocates will have control over the personal data collected by IoT companies if explicit consent is necessary before data collection. Respecting their privacy allows users to use IoT devices without apprehension regarding how their data is acquired and utilized. In addition, this may enhance consumers' trust in the companies since the companies will be viewed as upholding moral authority in data management practices. On the other hand, allowing IoT companies to gather information from consumers without their request may also abuse the consumers' privacy as the information may be misused or even leaked through data breaches.

Student Position

They affirm that consent mechanisms should be in place whereby users of IoT services must give authorization for their data to be retrieved and kept. Privacy is a fundamental right, and there has to be autonomy over the methods by which one's data is taken its meaning, and what the data will be used for. Collecting data promises additional advantages, such as improvement of services and products. However, the advantages do not suffice to compromise users' privacy. Companies need to be open and ethical in their operations so that the autonomy and rights of individuals are not abused.

The position is believed to be the most popular among orders and privacy advocates. The argument is that people's privacy and autonomy have to come first and that IoT companies have an ethical responsibility to observe these rights. Deontological ethics uphold this position, as it prescribes that actions should be assessed according to duty and not intention. Therefore, in this instance, IoT manufacturers, while doing so, should also hold individuals' right to privacy, even if it means going low on some degrees of convenience or speed of adoption of the technologies.

This approach is developed to guarantee that users get the relevant information and make decisions about managing their data.

It is recommended that IoT companies introduce tighter personal data protection policies requiring users' willingness and complete understanding before collecting any of their personal information. All such policies should provide an easy way of participation and withdrawal and be entirely explicit on the purpose of the information. Further, firms ought to step up the mechanisms in place for data protection to eliminate losses and exposure of personal details. This addresses the practical way forward regarding advancement and the social responsibility of every person to respect privacy. There has been so much emphasis on letting IoT Companies invent more solutions addressing ethics inside ecosystems to protect their users’ rights.

References

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things Security: A Survey. *Journal of Network and Computer Applications, 88*, 10-28. https://www.sciencedirect.com/science/article/abs/pii/S1084804517301455

Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications, 58*(1), 49-69. https://doi.org/10.1007/s11277-011-0288-5

Herold, R. (2020). Five Common Privacy Problems in an Era of Smart Devices. *ISACA Now Blog*. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/five-common-privacy-problems-in-an-era-of-smart-devices

Schneier, B. (2018). *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. W.W. Norton & Company.

Tene, O., & Polonetsky, J. (2013). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online, 64*, 63-69. https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2018). Privacy in the Internet of Things: Threats and Challenges. *IEEE Internet of Things Journal*. https://doi.org/10.1002/sec.795