DATA PRIVACY

THE UTILITARIAN AND DEONTOLOGIST PERSPECTIVES

ESTHER ABIODUN OSIKOYA

KNOWLEDGE LANGUAGE AND REPRESENTATION SHORT ESSAY

30/01/2024

Data Privacy: The Utilitarian and Deontologist Perspectives

1. Introduction

The meteoric rise in technology, the constant evolvement of new technologies like Drones, Wearable sensors, Network sensors, and Smartphones, to mention a few, among the Internet of Things devices, and their capability of revealing much about us to both strangers and close acquaintances with or without our permission has led to so much concern about the subject Data Privacy.

Although much focus has been on individual informational privacy, this essay will briefly discuss group informational privacy alongside individual informational privacy, as it could also affect an entire group if not adequately managed. Government agencies, Big Data organizations like Google and Facebook, to mention a few, and digital-related agencies have, over time, increased the rate of personal data collection from individuals. Although the availability of this data has, over time, helped in their decision-making and increased the development of different products, we must recognize the disadvantage of it. Hence, there will also be a brief discussion on the upsides and downsides of data privacy in section two of this essay. Since there has been so much debate on how the data provided by an individual should either be extracted with or without their consent over the past century, this spurred our interest in looking at the normative-ethical, theoretical perspective on the discourse, with a focus on the Utilitarian theory and the Deontologist theory and how it applies to Data privacy, this would be our focus in section three. We end the essay with a short conclusion to the discussion.

1.1 A Brief on Data Privacy

Lynch, in his book The Internet of Us, explained how the invention of the Kodak camera being used to take photographs of celebrities in a detrimental situation led to the publication of the article on 'the right to privacy' by Samuel Warren and Louis Brande in the late nineteenth century. This publication led to many debates regarding privacy, from finding the clear distinction between private and public to arguments on many debates regarding privacy across very different fields of society. Various critiques have given their views on the concept of privacy. One of these is the communitarian critique, which argues that privacy should not be seen

primarily as an individual's right to self-determination in physical or sexual matters. Instead, it should be viewed as protection given to practices that rely on being kept hidden from the view of others. Roessler (2001 [2005]), in her literature, suggests that three dimensions of privacy should be identified, namely decisional privacy, informational privacy, and local privacy, meaning the traditional "private sphere", mainly the home (the place, as opposed to information or actions). The dimension of informational privacy secures a wide range of expectations regarding what others know about him that is necessary for his autonomy, as "autonomy of decision is part of what it is to be a fully mature person", according to Lynch. The essentiality of this dimension of privacy among the three listed by Roessler leads to the discussion on individual and group privacy in the next section.

1.2 Data Privacy

Experts in diverse fields have informed us that data is not information but the raw material needed to have information. Access to a person or group's data may give us much information if appropriately mined. Hence, we conclude here that while Informational privacy and Data privacy are used interchangeably, we want to say here that informational privacy may encompass a broader range of personal information, including not just digital data but various aspects of an individual's private life, Data privacy often focuses on the secure handling of raw data, especially in the digital realm, ensuring that it is collected, processed, and stored in compliance with privacy laws and regulations. General Data Protection Regulation (GDPR) defines Data privacy as empowering users to decide who can process their data and for what purpose. A concern that has to do with not only individual data privacy but also group data privacy.

1.3 Individual Data Privacy

Over the past years, research and focus have been on individual informational privacy, an important area to investigate. Every positive and negative effect caused by any provided data can be traced solely to an individual. Lynch said in his book, "The more I know about you and the less you know about my knowledge, the easier it could be for me to take advantage of your ignorance: and the easier you will be to control or exploit." So, one reason privacy is important is that invasions of it can lead to exploitation, manipulation, and loss of liberty. Preserving individual privacy is crucial for maintaining personal autonomy, fostering trust in

relationships and institutions, and upholding the dignity and rights of individuals; for example, an employee expects that their personal information, salary details, and performance reviews will be handled confidentially by their employer. If performance reviews or other sensitive information is mismanaged, it can impact the individual's professional reputation within the organization. Colleagues and supervisors may form negative opinions based on disclosed information. This effect is not limited to the organization; mishandling personal information may compromise employees' security, including the risk of harassment, stalking, or other safety concerns if sensitive details are disclosed to unauthorized parties. It is an ongoing and evolving consideration, especially in the face of technological advancements and changes in societal norms. This development has to do with not only individual data privacy but also group data privacy.

1.4 Group Data Privacy

Research on group privacy addresses the fact that it is not individuals that are targeted by data collection and profiling practices, but rather groups of individuals who share certain relevant features, a common practice among Machine learning experts when working on data to get meaningful insight that either contribute to more intrusion of a specific group of people or the protection of their group privacy. With ever-greater frequency, privacy-invasive technologies have been argued to endanger individual interests and affect society and social life more generally. Therefore, the protection of individual freedoms and the constitution and regulation of social relationships are essential to privacy norms (see Roessler & Mokrosinska 2015). Group privacy refers to protecting the privacy interests of a collective or a group of individuals.

Several scholars have taken necessary steps toward developing a social approach to privacy in recent years. Arguing that a critical aspect of the significance of informational privacy is that it goes beyond the interests of the individuals it protects, these scholars have emphasized how privacy enables social and professional relationships, democratic decision-making processes, and political participation. They have also stressed the necessary role of privacy for cooperation and trust within various associations, such as economic partnerships. Regan, Solove, and Nissenbaum also follow this line of thought. Famously, Regan argues that privacy is not only of value to the individual but also to society in general. For Regan, privacy is a shared, public, and collective value (1995: 213; see Regan 2015: 50; Hughes, 2015). Solove claims that by understanding privacy as shaped by the norms of society, we can better see why privacy should not be understood solely as an

individual right; the value of privacy should be understood in terms of its contribution to society. (2008: 98, 171fn)

Multiple healthcare institutions collaborate to share anonymized patient data for research and development purposes. Group data privacy concerns involve implementing robust anonymization techniques to protect individual identities while enabling joint research efforts. Recently, a US healthcare organization filed a lawsuit for a data breach, a violation that affected almost 4.5 million individuals(Steve Alder, 2024). This is one of many examples where access to people's sensitive data is placed at risk because of data mishandling by organizations; this leads us to know the downsides and upsides of data privacy in the next section.

2.1 Upsides of Data Privacy

Knowledge, they say, is power, and power, when properly used, gives more freedom to its users. Data, as described by Lynch in his book, is a great source of knowledge, which in turn makes the primary owner more potent than a person who lacks access to it, as "autonomy of decision is part of what it is to be a fully mature person." as noted in by Roessler in her book, Privacy, that norms of informational privacy allow people to control who knows what about them. The knowledge others have about us shapes how we can present ourselves and act around others. Informational privacy is thus essentially linked to individual freedom and autonomy since it enables different forms of self-presentation and social relationships (see Roessler 2001 [2005: 111–141] for more detail).

Data privacy has many positive impacts, as seen in Big Data organizations, such as how constant mining of individual and group data has led to the development of several technologies and products, making activities and information more accessible and more efficient. Targeted ads can help make appropriate products available, and exploring them can help solve several group-specific problems. This good example shows the importance of taking advantage of group data.

Strong data privacy measures have enhanced trust in online activities, such as a secure environment for e-commerce, digital communication, and other online activities.

Privacy protection is crucial for protecting sensitive categories of data, such as health records, financial information, and other personally identifiable information, ensuring the confidentiality of such details. Unrestricted access to such data could lead to chaotic and uncontrolled consequences.

Lastly, Data privacy empowers individuals to have control over their information, allowing them to make informed choices about how their data is collected, processed, and shared.

As connectivity increases access to information, it also increases the possibility for agents to act based on the new sources of information. When these sources contain personal information, risks of harm, inequality, discrimination, and loss of autonomy quickly emerge; hence, we consider the downside of Data privacy in the next section.

2.2 Downsides of Data Privacy.

We have seen how proper access to individual and group data has fostered Innovation, research, and development. Strict data privacy regulations may limit organizations' ability to use data for innovative purposes, potentially hindering advancements in technology and research, which in turn affect every other part of society. Excessive regulation in the name of data privacy could stifle Innovation and create a climate of overregulation, potentially hindering the development of beneficial technologies and services. AI systems often rely on vast amounts of data for training and improvement; strict data privacy measures may limit data availability and diversity, affecting AI technologies' development and effectiveness as Innovation, research, and development are the heartbeat of a growing society.

We have seen so many cases where the availability of devices like CCTV cameras has helped law enforcement agencies combat both domestic crime and public crime. Aside from the fact that it exposes the perpetrators, it helps people comport themselves once there is awareness of this device in an environment; hence, excessive data privacy measures can make it challenging for law enforcement agencies to access crucial information for investigating and preventing cybercrime, hindering efforts to ensure public safety.

The global pandemic that occurred in 2020 would have claimed more lives than the documented number if there were stringent policies on data privacy to search for the root of the cause and likely measures to curb the further spread of the virus. Stringent data privacy regulations pose challenges to public health research by limiting access to large datasets, potentially hindering efforts to address health crises or conduct epidemiological studies.

Striking the right balance between individual privacy rights and broader societal interests, such as public safety and security, can be a complex ethical challenge that requires careful consideration and nuanced approaches. Hence, we consider the Deontologists' and Utilitarian perspectives in the next section.

3. The utilitarian and Deontologists perspectives on data privacy

Although the availability of data has, over time, helped in decision-making and increased development, there has been so much debate on how the data provided by an individual should either be extracted with or without their consent over the past century; this spurred our interest in looking at the normative ethical, theoretical perspective on the discourse, with a focus on the Utilitarian theory and the Deontologist theory and how it applies to Data privacy.

3.1 Utilitarian Perspective on Data Privacy

In his book, "Consequentialism", Walter discussed a diverse range of Consequentialism, which in turn stated an essential aspect of Utilitarianism. He stated that Classic Utilitarianism is a consequentialist theory, and it denies that moral rightness depends directly on factors other than consequences. Prof, Giorgio in his lecture note 'What is Epistemology ?', stated clearly that according to Utilitarianism, it is ethically right to do whatever maximizes utility for the highest number of people, which by implication means that if extracting individual data and group with or without their consent would be of maximum benefit to the society, then it is plausible to go ahead with the extraction and its mining for the betterment of the society. Although Walter, in his book, stated different forms of Utilitarianism, including Preferential Utilitarianism, Ideal Utilitarianism, and Utilitarianism of right, to mention a few, our attention in this subject matter of data privacy is also drawn to the Utilitarianism of right, where he claimed that one could hold that an act is right if it maximizes fulfillment (or minimizes violation) of certain specified moral rights.

Utilitarian theory frowns at unnecessary strict rules on data privacy, as this might cause harm to society; for example, a utilitarian would argue that it is morally wrong to keep strict rules on data privacy if the availability and extraction of such data would save the world from being affected by the wide range of viruses that are killing many at the moment or like at the future possibilities of the wide spread of the virus to eradicate a country if proper measures of it are not put in place.

The real-world problem is quite complex, making the theory of Utilitarianism a complex one as well; the statement of not placing a stringent rule on data privacy is entirely contextual as this might only work out in

some situations. For example, if placing strict rules on data privacy would protect a wide range of society from exposure to theft, insecurity, death, and other possible harmful consequences, the theory of Utilitarianism encourages the nondisclosure of such information. For example, it is morally wrong to give a house address to a stranger if disclosing it would lead to security threats and impose risk on the entire community.

The suffering in society would not have been minimized if the introduction of technologies and technological advancements had not been forthcoming. This evolvement of technologies is a data-driven practice. A utilitarian would argue that it is better to allow excessive availability of such data for the digital-driven organization since the availability of it would maximize utility for the highest number of people in society. A good example is the availability of life-saving machines that have been introduced to different healthcare sectors, that have, over time, combated health problems that had seemed impossible over the past centuries, an act that prioritizes the overall good health of people and minimizes the death rate in the society.

Although our focus in this essay does not cover the downside of this practice, we must say here that the complexity of life situations might make us selective in the kind of theory we adopt for diverse situations. Hence, we must consider another normative moral theory to help us know the practice that answers every view. So, we consider the Deontologist theory in the next section.

3.2 The Deontologist Perspective.

Alexander, Larry, and M

ùichael Moore, in their book, "Deontological Ethics," gave the different forms of Deontologists theory with their several strength and weaknesses, but in a more general case, as stated in What is Epistemology lecture note by Prof Giorgio, Deontology theory and practices have to do with what is consistent with some absolute duty or value. So, Deontologists offer a unique perspective on data privacy that centers around moral duties, rules, and individual rights. This theory does not focus on the maximization of utility as Utilitarian emphasized.

As a result of their stance on moral values and individual rights, Deontologists give maximum respect to individual rights and data privacy. In the discourse of data privacy, this means acknowledging individuals' rights to control and protect their personal information. Deontologists argue that privacy is not just a means

to an end but a fundamental right deserving protection for its own sake. Judging from this perspective, I may decide not to let out my details for some vital use if my moral value is to keep whatever is private to me, as this moral stance does not focus on the consequence of my actions but solely on my privacy.

As Alexander, Larry, and Michael Moore stated in their book, "Deontological Ethics," specific actions can be right even though they do not maximize good consequences, for the rightness of such actions consists in their instantiating certain norms (here, of permission and not of obligation). Deontologists stress the importance of fulfilling duties and promises. If a firm has made agreements regarding the privacy of individuals' or a specific group's data, a Deontologist believes there is a moral duty to keep these promises. A perspective that believes that promises and commitments create moral obligations and breaking them is ethically wrong, irrespective of potential positive consequences.

Avoiding the exploitation of individuals through the unauthorized use or disclosure of their data is another critical concern for deontologists. The true nature of deontological ethics is a commitment to respecting individuals' autonomy and protecting against exploitation; this includes protecting individuals from the misuse of their personal information for purposes contrary to their interests. Here, the Deontologist argues that if my agreement with a firm is solely to process my data for the development of a new product in the organization, it would be ethically wrong to process my data to perform prescriptive analysis for a widespread disease that is claiming lives, as the major concern is on the moral and not the consequence.

Conclusion

The world in its real sense is complex, which makes the best theory to choose about Data privacy a complex one. Hence, the answer to which practice is best depends on the type of perspective we view the subject matter. The complexity of data privacy has not in any way tampered with its necessity and the movement of keeping it intact despite the fast-growing developments in Research, Innovation, and Technology. Hence, both stances on data privacy must be considered, but there is a need for a meeting point between these two theories to draw a precise balance about data privacy. Whether prioritizing consequences or moral values about data privacy needs to be answered to avoid conflict, a resolution we are unsure of its possible outcome.

References:

1. Michael P. Lynch, “The Internet of Us - Knowing More and Understanding Less in the Age of Big Data”, W. W. Norton & Company, 2016.
2. Giorgio Lando, “What is Epistemology and why you should study it ?”, Knowledge Language and Representation, 2023.
3. Roessler, Beate, and Judith DeCew, "Privacy", ***The Stanford Encyclopedia of Philosophy*** (Winter 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.), https://plato.stanford.edu/archives/win2023/entries/privacy
4. van den Hoven, Jeroen, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, "Privacy and Information Technology", ***The Stanford Encyclopedia of Philosophy*** (Summer 2020 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/sum2020/entries/it-privacy
5. Sinnott-Armstrong, Walter, "Consequentialism", ***The Stanford Encyclopedia of Philosophy*** (Winter 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.), https://plato.stanford.edu/archives/win2023/entries/consequentialism

6. Alexander, Larry and Michael Moore, "Deontological Ethics", *The Stanford Encyclopedia of Philosophy* (Winter 2021 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/win2021/entries/ethics-deontological