

Ankit Tumuluri

Dr. Carl Cotner

Data Science 300

13 October 2024

Exercise 2: Public policy for data privacy and anonymity

Data privacy and anonymity are important issues in the digital age, as more and more information is collected, stored, and shared online. Megacorporations like Google and Meta have strategically convinced society to sign away their data and privacy, and so people today live oblivious to the fact that they are being monitored at every instant, while the corporations get richer and more powerful. Also, Data breaches are an all too common occurrence these days, with millions of people's sensitive passwords in the hands of malicious entities. Because of all these issues affecting today's information-reliant society, government laws and regulations are required to protect the public from the danger megacorporations have put society in. In this paper, I will analyze and discuss what kind of laws I believe should exist to protect the data privacy and anonymity concerns society has been facing and why I believe the laws are necessary in relation to information theory and how humans make decisions.

Humans make decisions based on the information they have and the information they expect to receive. They also have preferences and values that influence their choices. People are not always rational or consistent at all in their decision-making, they may be influenced by factors such as biases, emotions, and social norms. There is also a wide range of how educated the average person is on data security and privacy. Do they even know this is a serious problem? According to a report by Pew Research Center, "Americans are less knowledgeable about data privacy laws today than in the past. Today, 72% of Americans say they have little to no

understanding about the laws and regulations that are currently in place to protect their data privacy. This is up from 63% in 2019. By comparison, the shares who say they understand some or a great deal about these laws decreased from 37% in 2019 to 27% in 2023.”¹ This data clearly shows that the general public is not capable of governing itself and government action is desperately needed. Laws and regulations are desperately required to defend the public from a danger they are largely unaware of.

To ensure data privacy and security, detailed laws and regulations must be passed to regulate the collection, processing, and storage of personal information. These laws should mandate companies to obtain clear and obvious consent from people before collecting their data, ensuring there is transparency about the purposes of data usage. Additionally, these laws should require the implementation of nearly impenetrable security measures to protect against data breaches and unauthorized access. In 2023, new laws were passed in many states guaranteeing rights to individuals. These rights include: “the right to request access to inspect their personal information . . . the right to request that their personal information be deleted . . . the right to decide whether their personal information may be sold or whether it may be used for purposes of receiving targeted advertising . . . a guarantee that personal information should be used with informed consent from the data subjects, in a way that is understandable to them, and only for legitimate uses allowed under law, . . . and in the event of data breaches, a tested incident response plan should be in place to ensure that appropriate notifications can be delivered in a timely manner.”² These were massive steps forward for the United States in regards to data security and privacy. But this was only a select few states and more can still be done.

In today’s digital age, people are constantly at risk of having their identities compromised. Anonymity protection laws are crucial to prevent unauthorized access to sensitive

data that may greatly seep into personal lives. These laws should establish clear boundaries on data retention periods, limiting the storage of personally identifiable information to the minimum necessary for the intended purpose. Moreover, the laws should require organizations to adopt techniques to dissociate data from individual identities, enhancing overall anonymity. The right to erasure is also crucial in addressing this issue. This means that individuals should be able to request the deletion of their personal data once it is no longer necessary for the purpose it was collected for. This idea aligns with the concepts taught in information theory, which state that data loses relevance over time, and retaining it unnecessarily poses an increased risk of privacy infringement. There also should be laws that require organizations to provide clear and concise information regarding data collection practices. Individuals should be informed about the consequences of sharing their data which allows them to make informed decisions. This is related to a concept in human decision-making, which states that individuals often make decisions based on available information at their disposal. More information given to the individual reduces entropy and therefore a more suitable and predictable decision is likely to be made. Laws alone are insufficient without effective enforcement mechanisms. Stringent penalties for non-compliance should be implemented to incentivize organizations to follow the data privacy and protection regulations. This not only serves as a deterrent against negligent data practices but also reflects the importance society places on preserving individual privacy in the digital scene.

In conclusion, the establishment of thorough laws and regulations to protect data privacy and anonymity is paramount in today's digital landscape. The general public is still largely unaware of the danger they are in. Many do not know where their data is going and that it is falling into malicious hands time and time again due to a lack of pressure on companies and data

breaches. This is why the government must take matters into its own hands and pass specific laws and regulations to protect its people. These laws, which are grounded in information theory and human decision-making concepts, should address the collection, processing, and storage of personal information. By incorporating provisions such as the right to erasure and ensuring that informed decision-making is forced upon the public through transparency from the companies, government regulations can effectively balance the need for innovation with the preservation of individual privacy. These are the changes in laws and regulations that should exist to protect the data privacy and anonymity concerns that megacorporations have placed upon today's internet-reliant society.

References

1. [https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-d
ata-and-digital-privacy-laws/](https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/)
2. [U.S. data privacy laws to enter new era in 2023 | Reuters](#)