Intro (conception of privacy)

People right to privacy and the safety of their private lives is to be respected. They place a high value on having some say in who learns about them and most certainly don't believe anybody should at any point approach their own subtleties. Nonetheless, new improvements in data innovation put protection in danger, diminished how much command over confidential information, and made it more probable that admittance to individual information could have different horrible impacts. Data protection regulations were enacted in the second half of the 20th century as processing of personal data increased. (Van den Hoven, J. *et a,* 2019)

The value of privacy

Privacy is a crucial aspect of human dignity and plays a vital role in maintaining healthy relationships between individuals. However, the invasion of privacy is not new and can take various forms. Technological innovation poses a significant danger to individual and societal privacy, which is often overlooked due to society's eagerness for recent technologies. Regardless of the motivation for invading privacy, it harms both individuals and society.

Data protection is the appropriate handling of confidential information, including personal and financial data as well as intellectual property data, to comply with regulations and safeguard the confidentiality and integrity of the data with objective to maintain the immutability and availability of critical business data, with the protection of personal and sensitive information being a key aspect of this process.

Morals

According to Van den Hoven, J. *et a,* (2019) There are a variety of moral justifications for protecting personal data and giving individuals direct or indirect authority over how others can obtain that data, including the following:

Harm prevention: If others have unrestricted access to the data subject's bank account, biography, social media account, cloud repository, characteristics, and whereabouts, a variety of methods can be used to harm them.

Informational inequality: The use of data is becoming like the trading of commodities, where partners cannot ensure that contract terms are followed or negotiated. Data protection laws aim to provide assurance, ways to monitor compliance, and fair conditions for exchanging personal data. Technologies like access to information and marketing choice modelling take advantage of the imbalance of information between those in charge and those acting on their behalf.

Discrimination and injustice in the media: When personal information is used in one context, such as health care, it may have different meanings and effects in another, such as commercial transactions. Discrimination and disadvantages for the individual may result from this.

Abuse of human dignity and moral autonomy: When people's actions are exposed to others, they may lose their ability to make decisions independently and become influenced by external factors. Therefore, it is important to have regulations in place to protect individuals' personal information and give them control over how it is used. Businesses often use technology to ensure compliance with these rules.

Security is often the offspring of controversy. An American bank bought a hospital and used the medical records to foreclose on the debts of account holders with cancer. This shows the danger of medical data being in the wrong hands. Today, computer security is mostly about keeping hackers away from personal information. But what if those hackers are part of the system?

A simple 'cops and robbers' model Insufficient protection for data highlights the importance of securing it at various levels due to possible risks such as deterioration, falsification, loss, or leakage from internal, external, or random sources. One should view their connected system as a data stream and evaluate the potential dangers throughout the process.

### 

van den Hoven, J. *et al.* (2019) *Privacy and information technology*, *Stanford Encyclopaedia of Philosophy*. Stanford University. Available at: https://plato.stanford.edu/entries/it-privacy/ (Accessed: February 26, 2023).

Gavison, R. (1984) “Privacy and the limits of law,” Philosophical Dimensions of Privacy, pp. 346–402. Available at: <https://doi.org/10.1017/cbo9780511625138.017>. (Accessed: February 26, 2023).

<https://www.snia.org/educational-library?search=Data+Privacy&field_edu_content_type_tid=All&field_assoc_event_name_tid=All&field_release_date_value_2%5Bvalue%5D%5Byear%5D=&field_focus_areas_tid=All&field_author_tid=&field_author_company_value=&field_release_date_value=All&items_per_page=20>

https://ieeexplore.ieee.org/abstract/document/6227909

https://heinonline.org/HOL/Page?handle=hein.journals/lcp31&div=25&g\_sent=1&casa\_token=&collection=journals

Das, A.K. (2009) “An efficient random key distribution scheme for large-scale distributed sensor networks,” *Security and Communication Networks*, 4(2), pp. 162–180. Available at: https://doi.org/10.1002/sec.123. (Accessed: February 28, 2023).

Bélanger and Crossler (2011) “Privacy in the digital age: A review of information privacy research in information systems,” *MIS Quarterly*, 35(4), p. 1017. Available at: https://doi.org/10.2307/41409971(Accessed: February 28, 2023).