Intro (conception of privacy)

People respect their right to privacy and the security of their private lives. They value having some say in who can learn what about them. They most definitely do not want anyone to ever have access to their personal details. However, new developments in information technology put privacy at risk, reduced the amount of control over personal data, and made it more likely that access to personal data could have a variety of unfavourable effects. As the amount of processing of personal data increased in the second half of the 20th century, data protection laws were implemented. (Van den Hoven, J. *et a,* 2019)

The value of privacy

Concerns about adverse impacts are valid, as evidenced by the disclosures of Edward Snowden and, more recently, the Cambridge Analytica case (Cadwalladr & Graham-Harrison 2018). Government agencies and business actors use these technical skills on a regular basis to gather, store, and explore vast amounts of data related to phone calls, internet queries, and electronic payments. Many people's concerns have only grown as a result of China's ascent and the widespread use of cutting-edge digital technologies for monitoring and control. Personal information about current and prospective clients is now a valuable resource for businesses. (Van den Hoven, J. *et a,* 2019)

The debate over privacy is closely intertwined with the use of technology. The paper that started the discussion about privacy in the Western world argued that people have a right to privacy, based on the principle of "inviolate personality." Since then, the debate about privacy has been fuelled by claims about individuals' rights to control the extent to which others have access to them and claims about society's right to know about individuals. The development of information technology has been a major factor in the evolution of the privacy debate, and it is difficult to conceive of these concepts as separate from one another.

Data privacy is described as "information security that addresses data treatment in terms of permission, notice, sensitivity, and regulatory concerns." At its most basic, data privacy is a consumer's understanding of their rights around how their personal information is obtained, used, stored, and shared. Personal information utilisation must be communicated to customers in a plain and transparent manner, and in most cases, consumers must agree before providing their personal information.

Morals

According to Van den Hoven, J. *et a,* (2019) there are several different categories of moral justifications for protecting personal data and giving individuals direct or indirect authority over how others may obtain that data:

Prevention of harm: A variety of methods can be used to damage the data subject if others have unrestricted access to their bank account, biography, social media account, cloud repository, characteristics, and whereabouts.

Informational inequality: The use of data is becoming more and more like trading commodities, where individuals don't have the power to negotiate contracts or to check if partners are following the terms of the contract. Data protection laws, regulation and governance aim to establish fair conditions for transmitting and exchanging personal data, and to give data subjects checks and balances, guarantees of redress, and means to monitor compliance. These technologies, which exploit a basic informational inequality of principal and agent, are causing great disparities in access to information, choice modelling in marketing, micro-targeting in political campaigns, and nudging in policy implementation.

Informational injustice and discrimination: Using personal information in one context (for example, in health care) may lead to different meanings and consequences in another context (for example, in commercial transactions). This can lead to discrimination and disadvantages for the individual.

Encroachment on moral autonomy and human dignity: People who lack privacy are constantly exposed to outside factors that could affect their decisions, as they are aware that others are watching them. This can have a chilling effect on their autonomy and may lead to choices that someone without privacy would not have made.

These laws are designed to protect the privacy of people who are being processed by organizations. The principle behind these laws is that people must be informed about what is happening to their personal data, and they have the right to control how it is used. In addition, the data must be used for a specific purpose, and the person who is processing the data must be accountable to some kind of oversight authority. However, it is impossible to always comply with these rules, so companies often use "privacy-enhancing technologies" to try to protect people's privacy.

Security is often the offspring of controversy. A bank in the Midwest of the United States bought a hospital and its medical records a few years ago. It calmly compared the information to its own bank accounts and foreclosed on the debts of all account holders who had a cancer diagnosis. It was businesslike, straightforward, uneducated, and brutal, and an illustration of the harm that medical data can cause if it falls into the wrong hands. Nowadays, computer'security' is often understood to imply keeping hackers (those seeking unauthorised computer access) and other troublemakers away from your personal information. But what if these troublemakers are part of, or even own, the system?

Clearly, a simple 'cops and robbers' model does not provide enough protection, emphasising the significance of securing data security on several levels. Data deterioration, falsification, loss, or leakage can be caused by internal, external, or random dangers. Consider your connected system to be a data stream that flows from your keyboard to the recipient's, and assess the risks along the way.

### **The risks of connecting**

Open system internet

Connecting computers lets you to access other people's data, but it also allows others to access data on your own system. Unless individual computers or networks are brought together, they resemble 'islands' of electronic data. A data island's security is straightforward: reassuringly solid borders keep all unwanted intruders out. But, when it comes to constructing bridges via establishing a network link, this strategy is insufficient on its own. When a computer connects to the Internet, it loses its island status because the integrity of its 'borders' is jeopardised. The possible benefits of linking must be balanced against the hazards to your own data. This data is frequently particularly sensitive in a healthcare setting.

Closed system intranet

Why interact in such a public manner? Why not limit the connection to only 'friends'? In other words, why don't we simply connect to trustworthy computers over trusted network connections, therefore expanding our own trusted computing base? Go to the intranet. Intranets are best suited to smaller firms with rigorous security standards and staff management, which are not always possible in large health care enterprises. They are by definition limiting, as security by exclusion clashes with a network's ability to improve medical communications in a connected environment. Intranets may give the illusion of security: because the electronic thief attacks the weakest link in the chain, security solutions must reflect this. A well protected network requires closed terminal rooms, physiological checks for terminal access, and armoured, pressured wires to detect cable tapping.

virtual private network

A virtual private network (VPN) connects public and private networks by transferringprivate data via public networks like the Internet using a 'tunnelling protocol' and encryption (see below). Communication partners have no control over the network and no guarantee of service because they are not compelled to invest in a private network infrastructure. Until far, the most significant barrier to VPN implementation has been a lack of appropriate solutions.

Firewall

Just as you wouldn't allow someone to listen in on your phone call, you should take care of your Web surfing sessions and e-mail exchanges. A firewall, designed to protect your system, is required for this reason. These software or hardware devices work by detecting the IP address from which a message or system query is sent and allowing only those that are regarded as 'good' or trustworthy to get through. With the emergence of higher-risk 'always on' Internet connections, firewall solutions of different complexity are widely available.

van den Hoven, J. *et al.* (2019) *Privacy and information technology*, *Stanford Encyclopedia 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).

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).