Privacy Reflection Paper

BAN 220-NAA

Submitted by: Jasmeet Kaur

Student ID: 107154213

The World Health Organization (WHO) defines health as a total state of physical, social, and mental well-being. I consider privacy as *basic psychological need* which is very important for complete mental well-being in this digital era as securing privacy can ensure intellectual and psychic growth whereas privacy issues like information leak from a person's castle i.e., phone could cause anxiety and stress. However, as learnt during previous lectures on privacy, there also exist critiques of privacy who believe that everybody would be entirely honest if there exists *zero privacy* as there would be no deception. But privacy is a basic need yet for ones who have "nothing to hide". From the personal level information relating to an individual's financial accounts, health records, voting behaviour etc. to the national level data encompassing citizen's biometric records or classified files, privacy of information is required at every extent of society. This reflection paper aims to highlight the worth of privacy, assess modern risks associated with privacy in the digital age of big data and consider protection measures by various stakeholders.

So, what are the main sources that have access to our personal data? In the digital era, the data is collected at every level of individual interaction. Merchants and service providers, whether public or private like banks, healthcare institutions, government census records, employers, etc. are the reserves of personal information. This data gathering can take place on or off the web as apart from websites and social media, sensors might be present in personal devices, surveillance cameras or infrastructure, which can also track and collect data. Even if

these data do not represent private individual information, the bits of these data points can be collectively combined into information and information can be transformed to knowledge which can reveal personal sensitive information. As discussed during the lecture, mobile phones can reveal various amounts of private information about an individual through various features like location tracking, banking apps, cloud storage etc. For example, if the telecommunication company knows the location of a person, they may know the house of worship he/she visits and hence can know which religious denomination the individual belongs to. Therefore, the *sensitive information* of a person needs to be protected. But before discussing ways of information privacy protection, sensitivity needs to be defined with respect to data. According to me *sensitive information* can be defined as data that should be secured from illegal access and unwanted disclosure to preserve the information privacy and ensure security. Therefore, sensitive data comprises personal information, business data and classified information. Personal information includes data that can cause identity theft like Social Security Number, Health records etc. Sensitive business data consist of information that could cause a risk to the corporation if published to a competitor or public and classified information contains secret government data.

In present times, the big data is collected, used, and shared by the unknown entities that lack our trust. An individual is unaware of the vast possibilities in which their personal information can be used or misused intentionally or unintentionally by the organization and service vendor. Involvement of so many anonymous stakeholders is the main reason for me being not able to trust those with access to my private information. Also, there are also a growing number of instances of cybercrimes involving attacks like Pegasus even on encrypted and secure data. These incidents of cyberattacks can also make anyone sceptical of the privacy of his/her sensitive data. However, as awareness regarding the importance of privacy of information has grown, scandals like Facebook and Cambridge Analytica Data Scandal have

started coming to light. This incident has ended my relationship with Facebook as I deleted my account.

Next point to consider is that if there is fear of misuse of private information, should people refrain from disclosing their information? I don't think so. Big data sharing, collection and use is necessary to perform analytics and research, to improve service quality, to increase levels of customer service and to enhance revenues and therefore develop the economy. According to me, there exists degrees of privacy as it cannot be considered as complete non-disclosure of information, because privacy has different measures or levels of control associated with it. For example, although an individual's health records are personal to him/her, they are shared by a person with their health consultant to get appropriate care and treatment of a medical condition. But this sharing or discussion of health conditions with the doctor does not give him the permission or right to make these documents public. Therefore, there exists a measure of control with individuals over their health data. Now, let's expand this personal level example to a higher level of the world of data. Different private organizations, government agencies, service providers and merchants have considerable amounts of data about a person. This big data facilitates enhanced levels of customer satisfaction through adoption and evolution of technologies or services based on feedback and reviews. Since the data use and collection is helping me serve better apart from maximizing company's profit, I have no issues with these organizations using my data, but I am also against sharing my data with others or usage of my information in ways I don't approve of.

The next question is how to exercise different measures for the control of privacy? The legal contractual agreements are not a solution. For instance, this idea of everything or nothing is problematic in the case of consumer agreements that are required to be signed before using software or a website because usually, these contracts are written in such a way that requires us to give up control on the shared data. And consumers face a catch-22 of either giving up all

that control and get the service benefits, or not giving up control and therefore not getting any service. Therefore, I believe, the vendors of the services should provide graduated choices to users so the consumers can make the trade-offs they choose in points in the range that they're most comfortable with. For example, Google provides its users to surf in an incognito browsing mode. Typically, when a person is using normal browsing mode, the browser will remember internet sites that are visited by the user, and this helps the browser fill in entries into the search bar. It also helps to go back in history and revisit websites that they had liked after being navigated away from the page. Users may not get some services that they would get if they used normal browsing, but that's a trade-off that people can use in the manner they deem fit.

Apart from degree and measures of control related to privacy, another aspect to reflect about data privacy is the distinction between *collection* and use of *data*. According to me, the problem arises from improper and uninformed *use* of data. Collection is antecedent to use of data. Collection of data does not necessarily lead to any harm. An example, which was also quoted during the lecture on privacy, is surveillance by government or security cameras. Although security cameras do collect personal data, the purpose of data collection is to defer and deter crime, and that data is *used* only under certain circumstances like to catch shoplifters for example. Improper usage of data collected through surveillance can be guaranteed through appropriate government regulations at local, provincial, or federal level. Therefore, the government also plays an important role in ensuring the privacy of information of its citizens which is a precursor in ensuring data security. In the case of Canada, two federal level legislation offer privacy protections: the Privacy Act, applicable to the public sector, and the Personal Information Protection and Electronic Documents Act, which pertains to the private sector.

Therefore, in my opinion the loss of privacy occurs when there is a loss of control over personal data. Also, all stakeholders i.e., private organizations, the government, or individuals

themselves are responsible for ensuring privacy protection. Individuals must exercise their control over their data, service vendors whether private or public should provide options to consumers so they can exercise that control and government should formulate laws and regulations concerning proper use of data collected.

To conclude, privacy for me is both a basic need as well a basic right. The basic psychological need of ensuring privacy could be achieved through making it a legal human right. To ensure a secure feeling, protection of privacy is paramount. Therefore, privacy is fundamental to achieve security whether of the data or of the mind!