Should individuals have control over how organisations use their personal data

Sociology

Individuals Should Have Control over How Organizations Use Their Personal Data Personal data refers to any information about a person that can help in identifying the person easily. It refers to any data that is linkable to a specific person (Trinckes 2012) such as passport number, name, age, address, occupation, and telephone number among others. In addition, personal data may also include a person's insurance data (Hildebrandt, O'Hara and Waidner 2013), financial records, medical records, and even criminal records among others (Jarivs 2003). Notably, organizations do have access to personal data of their employees as well as that of their customers. Agreeably, personal data is very important and so individuals should have a role to play in controlling and protecting their personal data. Therefore, they should control what personal information organization gather and how they use it (Miller 2014). This essay presents an argument for control over how organizations use individuals' personal data.

Every person, employee or consumer, should have control over how organizations use their personal data. That is, they should have control over how organization collect, use, and disclose their personal information to assist them protect their privacy and any personal information that is shared. With increased cases of insecurity such as fraud, stalking and account hacking, every person has a responsibility to ensure that they control the kind of personal information they are disclosing. According to Personal Data Protection Act, the right of individuals to control their personal information should not be violated. In addition, this act allows individuals to request the organization possessing their personal data, be able to access, and amend their personal data. Organizations should also ensure that they get

individuals' consent to the collection, use and disclosure of their personal information. This requires an organization to inform people about the purpose of collecting, the use or disclosure of personal information. Moreover, individuals should also be able to withdraw their consent for collection, use or disclosure of their personal information by any organization at any time.

Arguably, the sensitivity of personal data makes it hard for organizations to keep individuals safe. Therefore, individuals' safety can also be ensured when they are able to control what information these organization access, use and disclose. However, they should be aware of the security risks that accompany the practice of sharing or disclosing personal information to any organization such as unauthorized access and use of their personal data. Some services such as providing a resume to an organization may attract identity theft because resumes contain sensitive personal information (Fischer-HüBner, et al. 2011).

Even though it is very important for individuals to have control of how organizations use their personal information, it is necessary to trust these organizations with such sensitive information especially if they have effective security measures to protect personal data that they possess. For instance, organizations should ensure that they prevent unauthorized access, use, disclosure or even modification of personal information of their customers. Moreover, organizations should not hold individuals' personal information for unintended purposes (Jarivs 2003). Some people are careless with their personal information, as they are not keen when they are sharing some sensitive information with others online. For this reason, organizations can

help protect their personal data from being accessed by stalkers and other criminals.

In conclusion, personal data is very important and sensitive and should therefore be used appropriately and disclosed whenever necessary so as to protect individuals. Customers have a right to manage what personal data organizations gather from them and control how they use such information and this will in turn ensures individuals' privacy and safety.

References

Fischer-HüBner, S., et al., 2011, Privacy and identity management for life 6th IFIP WG 9. 2, 9. 6/11. 7, 11. 4, 11. 6/PrimeLife international summer school, Helsingborg, Sweden, August 2 - 6, 2010, revised selected papers, Berlin: Springer.

Hildebrandt, M., O'Hara K., and Waidner M, 2013, Digital enlightenment yearbook the value of personal data. Amsterdam: IOS Press.

Jarivs, A., 2003, BTEC National for IT Practitioners: software development. Oxford: Heinemann Educational.

Miller, Roger, 2014, Cengage Advantage Books: Business Law: Text and Cases - The First Course, Stamford, CT: Cengage Learning.

Trinckes, John J., 2012, The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules, Florida: CRC Press.