ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 2, pp: (1-6), Month: April - June 2019, Available at: www.researchpublish.com

Digital Ethics and Privacy: A study about digital ethics issues, implications, and how to solve them

[1]Yasser A. AlQahtani, [2]Adel A. Marghalani

[1,2] Saudi Aramco, Information Technology (IT)

Abstract: **Information technology development has played a significant role in the collection and analysis of big data for better conclusions, but there is a significant concern in regards to privacy as an ethical concern. There is a deficiency of both legislation and ethics in the field of information technology due to the rapid growth and production of new IT products. The article seeks to establish the main issues and their implications on big data analysis, while at the same time providing solutions for the existing challenges. Collection of data without the informed consent of the owners, and the irresponsibility of various IT companies, has significantly jeopardized security and proper practice in the fast-growing industry. Most IT companies can bypass established restrictions through unclear privacy policies, taking advantage of the existing loopholes. Besides, the introduction of algorithms makes it easy for technology companies to create groups that have the potential of causing discrimination. Issues that are facing the IT industry and the use of products can be resolved by changing the consumers' behaviors and the technology producers. There is a lack of initiative by the companies to create ethical policies, which leave only the option of using legislation to force companies into compliance. Establishing and adopting more comprehensive digital ethical legislation and clarifying content-related ethical systems, can improve ethical compliance by the IT companies. Data science education can be introduced to curtail the ignorance of the public by making them aware of their privacy rights.**

Keywords: **Information Technology, Digital Ethics, Legislation, Privacy.**

1. DIGITAL ETHICS

Digital ethics refers to the study of the implication of technology on the social, political, and moral space of society. Capurro (2009) has extensively researched on the digital information and existing communication technologies implication on society at large. Currently, there is poor digital ethics practiced by IT companies due to the existing legislation gaps. There is minimal consensus on the moral and political philosophy investigations, with great dispute even on the basic digital ethics. The biggest challenge in digital ethics is the study of elements that cannot be seen with naked eyes, or which does not exist, with varying impacts and results on social morals and established traditions. Uncontrollable risks are inherent due to the uncertainty created by new technology, as well as the questions regarding new technology. Uncontrolled eventualities and outcomes in digital ethics are common, due to the inability to estimate the implications of different new technologies on society, because of the theoretical nature of the perceived outcomes (Floridi & Taddeo, 2016). For instance, the creation of artificial intelligence enabled computers, and interactive robots with human-like capabilities are increasingly becoming a reality, which requires new ethical standards. In society today, digital technology is more like what was previously featured in dreamlike science fiction literature, with technological applications in the social, political, and even moral spheres of life (Sargolzaei & Nikbakht, 2017). Due to new technology products, such as smartphones, the social sphere has become disrupted, with the most attention being given to online social relationships instead of real-life interactions. This article will assess the digital ethics environment today, to establish the challenges being posed by digital technology, to personal privacy and potential solutions to protect data.

2. DIGITAL ETHICS IMPLICATIONS ON PRIVACY

New information technology applications have led online interactions between people and even commerce, which has both positive and negative implications. Online interactions with individuals or online retail organizations lead to the exchange of a large amount of data, collected and analyzed by organizations for marketing and organization-based decision-making, without the consent of the owners (Sklavos, 2017). The inference created by mass data gathering through online interactions is a significant privacy violation, especially because most of the information owners are not aware of such activities. What is more worrying is that there is no clear ethical framework on digital technologies, which makes it difficult to deal with privacy and security concerns identified so far (Sklavos, 2017). This is because of the nonexistence of enabling legislation, and the rapid changes in the information technology environment. There is a need to address the privacy and security issues facing information technologies, to create solutions that ensure a safe digital environment for all the stakeholders. It is essential for the appropriate international bodies, to facilitate international binding legislation to help curb the growing cyber insecurity, such as cyberbullying and information loss, which threatens the positive implications of digital technologies.

Major Issues in Digital Ethics

The primary problems posed by modern technology to digital ethics is the violation of privacy by current big data analysis technologies, used by business organizations to improve their decision-making (Custers, Dechesne, Sears, Tani, & van der Hof, 2018). The aggregation data technologies are crucial in the collection of personal data, and there is a significant question of whether such activities by businesses are acceptable ethically, because the data is used to make decisions on marketing and production (Damen, Köhler, & Woodard, 2017). Privacy means any personal information regarding behavioral, financial, biometric, medical, and biographical data derived from business analytics. In this regard, it can be summarized that data analysis encroaches on personal privacy if it is used without the information owner’s consent (Bouguettaya & Eltoweissy, 2003). Although there is a privacy concern on how businesses collect private data, it is not necessarily unacceptable if the businesses seek consent from the data owners. In most cases, enterprises collect user data for use in improving their customer service by offering more personalized services and products (Richards & King, 2014). Some organizations request their consumers for confirmation on the collection and use of their data, and many leading organizations have used this model. Organizations, e.g., Google and Facebook, use the model to collect data to personalize consumer experience, but there is a rising claim of personal information abuse, such as sharing with third parties, e.g., the latest Facebook case for sharing consumer data with Cambridge Analytica, which used the data in geopolitical mapping (Schneble, Elger, & Shaw, 2018). Such cases undermine the morality of personal informed consent on the collection and use of personal data, due to the potential for abuse by companies.

Awareness of Data Management

Data management is the process of administering data by managing the acquisition, storage, validation, processing, and protection of data to ensure reliability, timeliness, and accessibility of data by the users (Bouguettaya & Eltoweissy, 2003). Technology advancements have been given precedence in society today at the expense of awareness of the privacy risks and issues surrounding the use of new technology. New technology applications, such as the Internet of Things, has been detrimental to data security and information management awareness, because of the forced consent of information owners without the knowledge of the sole purpose of the data collection (Tene, 2011). There is a lack of transparency by big data organizations, through the use of deceptive policies that help them to bypass the requirement for information owner consent. Besides, the autonomy of the individual information user makes it difficult to initiate any criminal proceedings against the technology giants, regardless of their abuse of private consumer data. There is indeed a considerable lack of knowledge regarding privacy policies by organizations and consumers, which has led to continued unethical practices by data-based organizations, such as collection of data without the owner’s consent (Clubb, Kirch, & Patwa, 2015). Besides, consumers have maintained a passive stance regarding their privacy rights, which has made it difficult to implement the existing privacy laws and requirements on owner consent (Steiner, Kickmeier-Rust, & Albert, 2015). It is clear that consumer behavior regarding privacy laws and consent, has been ignored due to a lack of awareness, and clear regulations to guide the public into making decisions on the requirements to share information. The poor compliance to protection measures is due to the lack of understanding of the potential risks posed by sharing personal data with information technology companies. There is a need for more awareness campaigns on the consequences and remedies for potential risks posed by new information technology practices, to protect privacy and improve data management practices (Riordan, Papoutsi, Reed, Marston, Bell, & Majeed, 2015).

Responsibility of IT Developers

The creation of infringing privacy information technology products and services have been blamed on developer negligence as well as the lack of awareness of the users, which makes it easy for the developers to overlook privacy measures (Clubb, Kirch, & Patwa, 2015). There is growing government involvement in ensuring developer compliance, which has led to the rejection of products deemed as infringing on the user's privacy, irrespective of their convenience, efficiency, and positive outcomes (Cate, Cullen, & Mayer-Schonberger, 2013). Besides the irresponsibility of certain profit-oriented organizations that infringe user privacy, there is a significant gap in policies, which makes it easy for IT developers to create services and products that do not meet the established safety standards. A developer has the responsibility of ensuring that they seek consumer consent during the collection of personal information. Governments should create legislation and regulations that curb developer malpractices, by ensuring that they maintain the consumer consent requirement (Custers et al., 2018). The developers also should shoulder the responsibility of creating awareness among the information technology consumers about their need to consent before sharing information.

Group Privacy

The emerging data analytic technologies are mostly focused on the behavior and lives of technology users with a high emphasis on anonymization with the aim of protecting personal information (Taylor, Floridi, & van der Sloot, 2017). The era of big data has enlarged the scope of data analytics with a significant focus being pushed on the group level, because data technology techniques have enabled the analysts to have greater access, which is a privacy threat. In the modern context, there is an increase in the privacy risk of groups in different social media platforms, which can be used in data analysis to place individuals in such groups, which results in adverse inferences that does not represent individual orientation, leading to discrimination against individuals in such groups (Taylor et al., 2017). This raises the need to establish a group-based privacy framework, which will suffice in such cases to protect the individuals from being discriminated due to group based orientations. There is need for further research to understand the privacy risk posed by social media analytics, as more algorithms are used to classify people in groups, which leads to specific conclusions and predictions without any actual knowledge of a person (Van den Hoven, 2017). For instance, being associated with a group can result in negative labeling, e.g., belonging to a group that is known to use drugs or engage in violent activities, which can result in detrimental profiling of individuals as being dangerous based on the grouping. This is an infringement to individual privacy, due to the unavailability of enough information to classify individuals in groups with most deductions being made in terms of demographics of the community, which individuals provide in their social media profiles as public information.

3. SOLUTIONS TO PRIVACY ISSUES

There are many diverse issues regarding privacy in information technology and new digital technology. The diversity of digital technology privacy issues makes it a challenge to create effective and efficient solutions (Bouguettaya & Eltoweissy, 2003). There is significant progress in the development of solutions, but the primary approach that can be used to control the cases of privacy infringement effectively is through the use of legislation to introduce new privacy policies. It is difficult to eradicate entirely unethical digital practices, even through legislations. Governments can enforce the law to a greater extent, which will significantly improve compliance.

Legislation Changes

The European Union (EU) countries have played a significant role in creating privacy guidelines that can be emulated by governments across the world (Custers et al., 2018). The primary approach through which the EU creates privacy guidelines is through the promotion of transparency, increasing individual participation, expanding developer accountability, data collection limitation and quality management, restriction, and safeguard-based measures. Through this legislation and principles in the creation of privacy policies, the EU has ensured that organizations comply with the data collection laws, especially by ensuring that the digital technology developers and users have the consent of the data owners (Custers et al., 2018). The EU ensures that the data owners are educated regarding the purpose of the information, and there is the need for developers to create secure databases for user information, which can be accessed by the owners. These measures have been crucial in ensuring successful measures reinforcement which can be significant in the creation of useful ethical guidelines (Har Carmel, 2016). Other legislation solutions include the requirement for complete transparency, device override capabilities, Internet of Things, dataset use control, and data protection. Therefore, such solutions infer that the government will play a more significant role in information management and security, and that consumers will be empowered to have control of their personal information.

Digital Technology Consumer Education

There is a need to create more awareness among information technology consumers on the privacy issues facing the use of digital technology (Serabian, 2015). Extensive education can incorporate digital technology users in the fight against information malpractice, such as the collection of information without the consent of the owners. Information education campaigns can be initiated for the public on information data handling procedures, which will equip the public with data safety knowledge to help minimize potential data loss (Kongnso, 2015). A well-executed education campaign can help to develop ethical literacy campaigns that can change the existing situation on data privacy, by increasing awareness on the right of the information owner to give consent before their information can be used (Clubb, Kirch, & Patwa, 2015). There is a limitation in that a limited period of education will not suffice in the eradication of data privacy concerns (Har Carmel, 2016). One of the methods of ensuring sustainability is the incorporation of data privacy education in the curriculums of education institutions, which will raise a data security practices aware generation that will act as ambassadors to educate those close to them, such as elderly parents and relatives who do not understand the data privacy concerns in digital technology applications (Matzner, 2018).Therefore, creating a sustainable education approach is necessary to sustain data security in society, amidst the growing use of digital information systems.

Responsible Innovation

Responsible Innovation is a term that owes its origin to the EU’s Framework Program, which seeks to encourage accountability among digital technology companies (Gurzawska, Mäkinen, & Brey, 2017). It was developed to describe the scientific research and technological development processes that would put into consideration the effects and possible impact on the environment and the entire society at large (Gurzawska et al., 2017). Therefore, Responsible Innovation is a transparent, interactive process through which the societal actors and innovators become mutually responsive to each other, with a view to the acceptability, sustainability, and societal desirability of the innovation process and its marketable products, to allow a proper embedding of scientific and technological advances in our society.

The core blueprint for the companies that focus their actions in the IT sector would be a deepened and critical focus on responsibility, which most likely should not deter their ability to formalize and implement the coveted progress in the technological space (Gurzawska et al., 2017). A scholar, Van der Hoven (2017), whose research focus on computer ethics, suggested a definition of Responsible Innovation that brings into account the accumulation of relevant knowledge on the options and outcomes, and their evaluation in terms of moral values, such as safety, security, and privacy, as critical requirements for the development of a new form of technology (Van den Hoven, 2017). The employment of these policies should be of utmost importance to both the consumers of that particular product, and the companies that are giving rise to them and. This is for the reason that the former would be more secure due to the more ethical consideration by the manufacturer, and the latter would encounter minimal hitches related to potential conflicts as required by the law or in case of a breach in the privacy requirements.

Group Privacy

New technologies tend to pose new challenges on the protection of privacy, and they also arouse new and profound debates on the scope of confidentiality. These debates always revolve around the individual's ability to control the flow of their personal information. Protecting the privacy of the group by using the policies that are explicitly outlined in legislation may prove to be a challenging task at times (Taylor et al., 2017). This is because the many groups that are derived by big data analytics are not specific components in the physical world. As such, real group privacy protection measures call for extensive and intensive joint research conducted by ethics specialists and information analysts.

There is a need to change the procedures and the methodology that is employed during significant data processing to be more conducive to privacy without significantly having post-effects on their performance (Taylor et al., 2017). Nevertheless, some measures, which primarily concentrate on improvement to individual privacy and the consequent partial reinforcement of its group counterpart, are possible to implement now. Taylor, Floridi, and van der Sloot (2017) established approaches, such as the international integration of data management regimes, improved data security and breach accountability, and enhanced data literacy. A centralized model where a user would be able to see the extension of their data, and determine the extent of the information use, would be optimal and commendable to promote consumer involvement and control of personal data (Taylor et al., 2017).

4. CONCLUSION

There is a continuous need for regular updating of data privacy legislation to meet the changing information technology environment privacy concerns. Governments should take the primary role in ensuring current legislation can tackle new and existing information security concerns. The lack of awareness and developer irresponsibility, and lack of compliance with established guidelines, continue to be major issues for digital information. Therefore, there is the need for a multidisciplinary approach to tackle security issues, such as education to create awareness of guidelines, legislation by the government, and increased developer responsibility towards compliance and creating user awareness of the necessity of consent, as well as other data security measures.

REFERENCES

[1] Bouguettaya, A. R. A., & Eltoweissy, M. Y. (2003). Privacy on the Web: Facts, challenges, and solutions. *IEEE Security & Privacy*, *99*(6), 40-49. Retrieved from https://pdfs.semanticscholar.org/032c/98dbf8ac0ea99943bf70175bf8bad99950a4.pdf

[2] Capurro, R. (2009). Intercultural information ethics: foundations and applications. *Signo y Pensamiento*, *28*(55), 66-79. Retrieved from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-48232009000200004

[3] Cate, F. H., Cullen, P., & Mayer-Schonberger, V. (2013). Data protection principles for the 21st century. [Internet Source]. Retrieved from https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf

[4] Clubb, K., Kirch, L., & Patwa, N. (2015). The Ethics, Privacy, and Legal Issues around the Internet of Things. *University of California-Berkley. Last modified Spring*. Retrieved from https://www.ischool.berkeley.edu/sites/default/files/projects/w231-internetofthingsfinalpaper.pdf

[5] Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, *34*(2), 234-243. Retrieved from https://www.bedicon.org/wp-content/uploads/2018/01/laws_topic7_source1.pdf

[6] Damen, J., Köhler, L., & Woodard, S. (2017). The Human Right of Privacy in the Digital Age. *Publishup.uni-potsdam.de*. Retrieved from https://publishup.uni-potsdam.de/opus4-ubp/files/39926/srp03.pdf

[7] Floridi, L., & Taddeo, M. (2016). What is data ethics? *Oxford Internet Institute*, University of Oxford, 1 St Giles, Oxford OX1 3JS, UK. Available from https://doi.org/10.1098/rsta.2016.0360

[8] Gurzawska, A., Mäkinen, M., & Brey, P. (2017). Implementation of Responsible Research and Innovation (RRI) practices in industry: Providing the right incentives. *Sustainability*, *9*(10), 1759. Retrieved from https://www.mdpi.com/2071-1050/9/10/1759/pdf

[9] Har Carmel, Y. (2016). Regulating' Big Data Education in Europe: Lessons Learned from the US. Internet Policy Review. Retrieved from DOI: 10.14763/2016.1.402

[10] Kongnso, F. J. (2015). Best practices to minimize data security breaches for increased business performance. *Walden University*. Retrieved from https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=2928&context=dissertations

[11] Matzner, T. (2017). Data science education as contribution to media ethics. In *Paderborn Symposium on Data Science Education at School Level 2017: The Collected Extended Abstracts* (p. 28).

[12] Richards, N. M., & King, J. H. (2014). Big data ethics. *Wake Forest L. Rev.*, *49*, 393. Retrieved from http://www.informatica.uniroma2.it/upload/2017/IA2/RIchards%20and%20King%20BigDataEthics.pdf

[13] Riordan, F., Papoutsi, C., Reed, J. E., Marston, C., Bell, D., & Majeed, A. (2015). Patient and public attitudes towards informed consent models and levels of awareness of Electronic Health Records in the UK. *International journal of medical informatics*, *84*(4), 237-247. Retrieved from https://doi.org/10.1016/j.ijmedinf.2015.01.008

[14] Sargolzaei, E., & Nikbakht, M. (2017). The Ethical and Social Issues of Information Technology: A Case Study. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, *8*(10), 138-146. Retrieved from http://thesai.org/Downloads/Volume8No10/Paper_19-The_Ethical_and_Social_Issues_of_Information_Technology.pdf

[15] Schneble, C. O., Elger, B. S., & Shaw, D. (2018). The Cambridge Analytica affair and Internet-mediated research. *EMBO reports 19*(8), e46579. Retrieved from https://doi.org/10.15252/embr.201846579

[16] Serabian, D. (2015). Consumer Protection and Cybersecurity: The Consumer Education Gap. The University of Nevada. Retrieved from https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1032&context=brookings_pubs

[17] Sklavos, N. (2017). Privacy in a Digital, Networked World: Technologies, Implications, and Solutions. By Sherali Zeadally and Mohamad Badra. *Springer International Publishing*: 418 pp.; $51.89; ISBN-10: 3319084690, ISBN-13: 978-3319084695. Retrieved from doi:10.3390/cryptography1010005

[18] Steiner, C. M., Kickmeier-Rust, M. D., & Albert, D. (2015, March). Let's Talk Ethics: Privacy and Data Protection Framework for a Learning Analytics Toolbox. In *Ethics and Privacy in Learning Analytics (# EP4LA)*. Retrieved from http://css-kmi.tugraz.at/mkrwww/leas-box/downloads/LAKEthics15.pdf

[19] Taylor, L., Floridi, L., & van der Sloot, B. eds. (2017). Group Privacy: new challenges of data technologies. *Dordrecht: Springer*. Retrieved from https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf

[20] Tene, O. (2011). Privacy: The new generations. *International Data Privacy Law*, *1*(1), 15-27.

[21] Van den Hoven, J. (2017). Ethics for the Digital Age: Where Are the Moral Specs? In *Informatics in the Future* (pp. 65-76). Springer, Cham. Retrieved from https://link.springer.com/chapter/10.1007/978-3-319-55735-9_6