Ethical Dilemmas

Privacy In The Digital Age: Information Privacy Does Not exist

ACCG8086

Author: Mohammed Sadiq Abuwala
Student ID: 45921407

Date: 25 / 05 / 2021

Introduction

The 21st century will undoubtedly be known for its rapid advancement in technologies. The world is becoming more integrated due to increased internet connectivity and access to advanced digital technologies such as IoT and Virtual Assistants. Today, information is seldom stored in physical papers. The medium of collecting and storing information has evolved. However, there still remains the risk of information being stolen and subsequently misused. It also becomes hard to understand the flow of information in complex digital technologies. This gives the view that information privacy may not exist. This paper aims to investigate ethical dilemmas relating to information privacy that arise due to the evolving nature of digital technologies. Finally, the author also discusses various frameworks that exist today to resolve issues related to information privacy in this digital age such as GDPR, COPPA, COBIT 2019, and the ACM Code of Ethics.

1.0 Information privacy

Information privacy (or data privacy) relates to the access, use and collection of data, and the data subject's legal right to the data. The concept broadly refers to:

- Allowing only authorized access to personal data.
- Allowing only authorized usage of personal data.
- Maintaining accuracy and completeness of personal data.
- A data owner's legal right to access, inspect, delete, update or correct these data (W. Lee, Zankl and Chang, 2016).

2.0 Requirement for Information privacy

The requirement of information is urgent and complex. We are rapidly inclining towards a world which is technology driven. A vast majority of these technologies operate in an information intensive environment. Some examples of such technologies are Virtual Assistants such as Apple's Siri or Google Assistant, Social Networks such as Facebook, and Search Engines such as Google. Users also benefit from these information intensive technologies because they are able to attain an experience that is more personalized / relatable to them.

Information privacy also introduces better transparency for users and organisations. It allows a consumer to be better informed and promote better trade practices between organisations.

Information privacy can also be viewed as a necessity. Digital technologies are constantly evolving. This leads to newer attack vectors constantly surfacing. Although a majority of the population are using these digital technologies to improve their quality of life, some individuals and organisations are using them to commit newer forms of crimes or traditional forms of crime more efficiently. For example, the advent of digital technologies such as printers have made it possible to commit identity theft more quickly and accurately. Therefore, information privacy can be considered as a necessity in order to deter crimes using digital technologies.

3.0 Society's view on information privacy

Different cultures put different values on information privacy. For example, the European Union enforces an information privacy mechanism known as General Data Protection Regulation (GDPR). It is an all purpose regulation that must be followed by all businesses operating in EU territory. In contrast, the US implements sector specific data privacy laws that may sometimes also be intertwined with state laws. Hence, a universally accepted definition of Information privacy does not exist but there is a general consensus on the broader concept of a person's right to privacy. For example, a person is not legally obliged to identify themselves while using traditional technologies such as during a telephone call. There exists a general consensus on this notion of information privacy and that it should in the same way apply to digital technologies.

Different individuals also put different values on information privacy. This could be due to an individual's varying morality or perception of privacy. For example, let us assume two employees (Alice and Bob) from the same cultural background who are working at an organisation. Bob may think that it is morally acceptable to take a confidential USB drive home in order to complete organisational activities. This is because he believes that the positive impact he will make towards the organisation's success by completing his assigned work far outweighs the negative impact caused by such an infraction. Furthermore, it is his perception that the likelihood of the USB getting lost or stolen is low. In contrast, Alice finds it morally unacceptable and does not want to take such a risk because of her perceptions and unique experiences.

4.0 Is this view of Information privacy maintained in developing countries?

In this section, we will examine a range of developing countries such as India and Bangladesh. Indian people tend to lose their concern about online privacy when gaining internet experience (Knopp, 2019). For example, the paper detailed a study conducted in which 60% of participants were unconcerned with the publication of traveler information such as full name, age, gender, seat number and departure station at a train station. The study further revealed that in comparison to US participants, their Indian counterparts were much more significantly comfortable in sharing their health records with others (India: 29%, US: 6%). It concluded that:

“Indian society has less concern and low awareness on their information privacy protection, as compared with Americans. The Indians have the inclination to believe that their personal information will not be misused and completely oblivious of the possibility of the personal information trading among companies, including their personal medical information. They have the attitude of willingness to share and trust the business organisation and government in handling their personal medical information but information privacy rarely exists in these cases” (Samsuri, Ismail and Ahmad, 2013).

Even the most traditional or basic forms of technologies such as the use of a mobile phone can become a privacy challenge in developing nations. For example, device sharing is a common occurrence in developing nations such as Bangladesh (Ahmed, Haque, Chen and Dell, 2017). The study details three such common occurrences. In one instance, devices may be shared between siblings. Devices may also be shared between husband and wife. Finally, a much more common occurrence is device sharing between parents and siblings. In a majority of such cases, there is a ‘family phone’ which is shared between the mother and the sibling while the father’s mobile phone remains private. This may seem like a beneficial scenario to all parties as each individual attains access to the technology and therefore benefits from its use. However, this introduces significant ethical dilemmas because it causes a major impact on gender dynamics and privacy violations. There is also a widely held opinion among low income families that privacy can only exist for upper-class families (Rowntree, 2018).

5.0 With current existing technology, is privacy even certain?

The 21st century will undoubtedly be known for its rapid innovations in technology such as deep learning, Robotic Process Automation (RPA) and Quantum Computing. The rapid evolution of digital technologies has led to a person having reduced control over their personal data and subsequently this has led to a range of negative consequences. This can be clearly seen when we examine recent events taking place in the world such as the Cambridge Analytica scandal and the revelations of Edward Snowden. Government agencies and corporations alike now possess the technological means to collect, store and process large quantities of extremely sensitive personal information such as internet searches, phone conversation details and electronic payments. Furthermore, it is even more concerning that such sensitive personal information is frequently used by government agencies and corporations alike (Cadwalladr & Graham-Harrison 2018). For example, China nowadays routinely collects, stores and processes personal information relating to its citizens and uses emerging technologies such as face recognition to conduct large scale surveillance. In the following section, the author discusses various current technologies such as IoT, E-Government Services and Digital Advertising to examine this notion further that privacy is uncertain with current technologies.

6.0 The Internet of Things (IoT)

Devices today are not just limited to traditional mainframe computers. In technologies such as IoT, devices are connected to the internet via technologies such as RFID, Bluetooth, NFC, Wireless sensor networks and LTE. The connectivity of these devices to the internet allows the transfer of gathered information and leverages the processing power already available over the internet. Therefore, the device is able to perform services based on its ability to transfer information over the internet and hence called as such (i,e, Internet of Things).

IoT devices automatically generate statistics in order to operate and this is usually sensitive personal information. For example, smart thermostats may collect statistics about preferred room temperatures and smart meters may collect statistics about a user's water consumption. In the future, we will see such technologies being incorporated in our daily lives more extensively as more and more smart technologies become integrated into household appliances.

Emerging technologies as such introduce new ethical dilemmas. Product designers should be more transparent about the associated connectivity of such devices. For example, IoT devices that employ a microphone may be of concern to a user. Transparency should be provided that such devices are not listening to a user's conversations unless it is known to the user or informed consent is provided. Such devices are capable of collecting big data about a user which is usually sensitive personal information. Yet, organisations are more concerned towards quickly releasing IoT devices in the market before putting sufficient security considerations in place.

7.0 E-Government

Government services around the world are undergoing radical transformation due to the availability of advanced digital technologies. This trend can be seen via examples such as the widespread implementation of biometric passports and e-government services such as mail voting. Let us examine the trend of the mail voting system in depth to get a view of the unique ethical dilemmas encountered via use of emerging technologies in e-government services. There is a general consensus that elections should occur via secret ballot in order to prevent voter buying or coercion. In a polling station, authorities are able to secure the location and ensure that a voter is not being monitored and is able to vote privately. However, law enforcement is not able to maintain such security when a voter is voting by mail or online. Hence, information privacy cannot be guaranteed. This shows that while such emerging technologies have provided citizens with additional ways to vote and improve productivity/participation, the resultant effect may actually be the erosion of information privacy. In cases such as voting, it is not only a right of the user to have information privacy but also the duty of the government to ensure that these rights are met. This is because in order to maintain and ensure a democratic environment, it is paramount to prevent undue influence.

8.0 Digital Advertising

The consumer's free choice is the foundation in consumer and advertising ethics. This ethical value is rarely granted when a consumer uses digital technologies nowadays. Initially, advertising was introduced in order to provide tailored information to the consumer which in turn would allow them to make better choices. However, the process today involves the use of complex algorithms based on various filters and corporate policies. The way these algorithms work are seldom known to the consumer. Thus, individuals lose control over the flow of information. Furthermore, they also possess insufficient knowledge about how their personal information will be used.

Advertisers do undertake measures to inform the users of ways in which they collect and process personal information but these measures are rarely sufficient. For example, We are keenly aware that requiring users to agree to terms and conditions does nothing to solve the problem (Becker, 2019). Users rarely tend to them. Furthermore, in the majority of cases, these terms and conditions only provide information about how personal data is stored and processed. It does not provide information about how an advertiser's algorithm operates. Hence, it becomes difficult to understand the flow of information and this leads to a loss in transparency.

There is also an empirical question as to what extent an advertiser's algorithms influence a user's behaviour. The original concept of advertising related to helping users make better choices. However, there is debate as to how much an advertiser should influence a user's decision. It could be considered unethical for an advertiser to possess significant influence over an individual's daily lives.

There is also a concern regarding the accuracy of the data collected by the advertiser. The services that advertisers show to the user are based on the user's web activity. However, a person's web activities may not always be related to a user's interest. For example, people surfing the internet often encounter news that they were not consciously looking for, but which they nevertheless take seriously. This is called 'inadvertent' attention for news (Becker, 2019). Hence, services promoted by advertisers based on these web activities may not be of interest to users and could even be regarded as a nuisance.

There are also times when it may not be suitable to show advertising based on a user's web activity because it may not be beneficial to the user. In such cases, the advertisers should not use this information even though they may have access to it. For example, there has been debate in Australia regarding the advertising of fast foods and soft drinks to an individual; especially children (Morton, Stanton, Zuppa and Mehta, 2005). Hence, this raises an ethical dilemma regarding when it is the right time to collect information about a user for the purpose of digital advertising.

9.0 Personal information used for research/product development

There are many organisations that use personal information in their research activities for product development. For example, Facebook conducted a research in 2014 on thousands of unwitting users. Their aim of the research was to deduce if showing positive or negative stories on a user's news feed produced a predicted emotional state. In essence, the organisation tried to manipulate a user's emotional state and it was considered to be disturbing and a gross violation of ethical standards (Kramer, Guillory and Hancock, 2014). In the offline world, we generally operate autonomously. However, this standard is not generally upheld when a user is online. One of the central discussions of information privacy relates to achieving improved transparency and clarity on the flow of information.

Several recent frameworks have attempted to encompass the subject of using personal information for research purposes. For example, the GDPR states that appropriate safeguards and freedom must exist for the user in the event that such personal research may cause substantial distress or damage to the data subject. Furthermore, the use of personal information should not be used to conduct research on a particular data subject unless it is for the purpose of approved medical research. The GDPR framework also notes that the concept of data minimization should be extensively followed. Data minimization means that the data should be used for the intended purpose only and also limited to what is necessary. Several frameworks around the world today emphasise on the principality of data minimization. Some examples of such frameworks are California Consumer Privacy Act (CCPA), and Brazil's General Data Protection Law.

10.0 How do privacy laws change for minors?

We have just discussed how special considerations should be taken when collecting and using information from minors. Now, let us examine how privacy laws around the world encompass this subject. Governments around the world recognize that children deserve special recognition in the context of data privacy and the internet. This can be noted in various privacy laws worldwide. Some examples of these are the General Data Protection Regulation (GDPR) and Children's Online Privacy Protection Rule ("COPPA"):

10.1 COPPA

“COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age” (Federal Trade Commission, 2002).

Various aspects are covered in relation to data collection and usage of minors. If an organisation runs a plugin or ad network that collects personal information about minors and the organisation is aware about this, they must comply with COPPA laws. Furthermore, even if a digital technology is directed towards a general audience but there is a probability that the audience may include minors, the organisation must comply with COPPA laws.

Even though it was introduced in 1998, it is routinely updated to keep up with emerging technologies. For example, it was updated in July, 2013 with several revisions. Henceforth, organisations were required to undertake reasonable efforts (taking into account available technology) to provide direct notice to parents of the organisation’s practices with regard to the collection, use, storage, or disclosure of personal information from minors under 13.

The COPPA privacy laws are known for its strict policies and improving data privacy for minors but it also introduced new ethical dilemmas. It is not known to be very effective outside US jurisdictions and hence does not entirely solve the issue of ethical data collection and processing of minors. The Federal Trade Commission (FTC) asserts that COPPA applies to any organization that directs their services towards the US. However, the FTC has never in practice enforced non compliance outside their jurisdiction. Efforts should be undertaken to come up with a general standard that operates in synchronization with other jurisdictions. Most jurisdictions around the world still have not implemented laws to enforce ethical data collection and processing of minors. For example, Australia’s Privacy Act of 1988 does not have any specific references to children.

Some organisations operating services directed towards the US are also choosing to ban minors aged below 13 entirely from their services. Some SMEs do this because they believe compliance would incur higher costs which they are not willing to undertake. These services may be safe for a child to use and may even be beneficial but the child is unable to use it. Thus, this introduces a new ethical dilemma as to why they are unable to access services to which they are rightfully entitled. Minors should not have lesser access to services than adults simply because organisations are not willing to undertake measures to protect data privacy of minors.

11.0 COBIT 2019 to support an appropriate organisational cyber ethics approach

COBIT 2019 was recently released as an update to the Control Objectives for Information and related Technology 5 (COBIT 5) framework. It was designed by the Information Systems Audit and Control Association (ISACA). The aim of the COBIT framework is to provide practical and comprehensive guidance to support enterprises in managing their information and technology. There are various new features proposed in the updated framework. However, the overall purpose of the framework remains the same and that is the governance of enterprise Information Technology (IT).

There are some notable features in the new framework which could help organizations in maintaining information privacy. For example, COBIT 2019 introduces the concept of Focus areas next to its generic government and management objectives. This introduces an open and flexible architecture that supports the creation of specific and detailed guidance on virtually any topic. Initially, focus areas will be available for SMEs for the purpose of attaining information security and information risk assessment (Harisaiprasad, 2021).

The author has discussed how individuals and organisations sometimes feel a loss of control over flow of information because of the complex methods by which these advanced technologies operate. The Data Management component (AP014) of the COBIT 2019 framework also seemed beneficial for organisations aiming to manage their data. This component allows an organisation to manage their data assets across its entire life cycle (i.e. creation, delivery, maintenance and archiving). In particular, its subsection APO14.01 (Define and communicate the organization’s data management strategy and roles and responsibilities) states that data management strategy must be communicated to all involved stakeholders such as the source and owner of data. Furthermore, it supports the management of corporate data as critical assets. We have also discussed how organisations such as digital advertisers should aim to maintain completeness and accuracy of collected information. The subsection, APO14.04 (Define a data quality strategy) supports an organisation in defining an corporate wide strategy to achieve data quality. By successfully implementing APO14.04, an organisation will be able to maintain accuracy and completeness of collected data. Furthermore, APO14.06 (Ensure a data quality assessment approach) provides a continuous approach to evaluate data quality.

Up until now, the author has discussed approaches to ensure that data collected is complete and accurate. Additionally, the updated COBIT 2019 framework also defines a mechanism (i.e. APO14.07: Define the data cleansing approach) to correct data according to predefined business rules.

There are various other notable components of the COBIT 2019 frameworks that allow organisations to maintain information privacy for itself and subsequently users alike. The subsection APO14.08 (i.e.Manage the life cycle of data assets) ensures that strategies are in place which allow an organisation to understand, map, and control the flow of data as it passes through its business processes. The flow of data is mapped from the time of data acquisition to retirement. The APO14.09 (Support data archiving and retention) ensures that data archiving and retention follow legal and regulatory requirements.

Initially, in the COBIT 5 framework, the APO14 component was known as ‘Align, Plan and Organize’. It was used to address overall organisational strategies and IT objectives. In the updated COBIT 2019 framework, this component was restructured and an additional objective (APO14: Managed Data) of this new structure was to achieve and sustain the effective management of an organisation’s data asset. This update was made because nowadays, there is an increased focus on privacy and stringent privacy legislations in several jurisdictions around the world (For example: Europe’s GDPR). Therefore, the COBIT 2019 framework also implements these concepts of data protection and privacy. By doing this, it is able to leverage and work in tandem with existing frameworks such as the GDPR and NIST cybersecurity framework.

The Deliver, Service and Support (DSS) component of the COBIT 2019 framework can also be aligned with our goal of attaining information privacy. The DSS02 (Managed service requests and incidents) subcomponent of DSS states that an organisation must enforce strategies which allow effective and timely response to user requests and resolutions regarding all types of incidents. The DSS02 subcomponent states that an organisation must put measures in place to record, diagnose, escalate and resolve incidents. Earlier in the report, the author has discussed the ethical requirement of allowing users the right to correct or totally erase related personal information. By successfully implementing DSS02, the organization will be able to respond and resolve user requests regarding personal information such as correction or deletion.

12.0 ACM Code of Ethics for dealing with cyber ethics

The Association of Computer Machine (ACM) Code of Ethics is considered as the standard for the computing profession. It is designed to guide technologists in making ethically responsible decisions. It is not an algorithm but a set of principles for ethical decision making. It was first introduced in 1992. However, in 2018, it was updated to keep up with the advancement of technologies. The ACM Code of Ethics does not explicitly mention any specific emerging technologies but uses implicit language to include all such current and future technologies. For example, it addresses recent developments such as the requirement for algorithmic transparency.

Principal 1.3 (Be honest and trustworthy) of the ACM Code of Ethics notes that a computer professional should be transparent (ACM Code of Ethics and Professional Conduct, 2018). Furthermore, it states that full disclosure should be provided to all concerned parties regarding system capabilities, limitations, and potential issues. This is certainly necessary in the context of emerging technologies such as IoT. This is because IoT devices employ a range of intrusive technologies in order to operate such as mic and cameras. These devices have the ability to record big data about a user which usually is sensitive personal information. Computing professionals should be transparent with consumers about the manner in which IoT devices operate. By following Principal 1.3, computing professionals can offer transparency about personal information collected, stored, and processed about a user.

The updated ACM Code of Ethics also aims to resolve the ethical dilemma of data collection. In Principle 1.6 (Respect Privacy), the concept initially revolved around opt-in and opt-out procedures in regards to data collection. However, in the updated ACM Code of Ethics, there is a move towards a more general requirement of informed consent procedures. Now, users must have the ability to consent or withhold consent, understand what data is being collected and also the reasons for which it would be used in the future. These updates make them consistent with current privacy legislations being implemented around the globe.

13.0 Organisational response to ethical dilemmas posed by emerging technologies

The author notes that the ACM Code of Ethics provides computing professionals with a general guideline on the code of conduct. However, no specific guideline is provided based on the type of technology. Hence, there are instances where the ACM Code of Ethics may be insufficient. For example, Principal 1.3 of the ACM Code of Ethics states that a computing professional must strive to be honest and trustworthy. However, it is difficult to anticipate ethical issues that may occur with new technologies. Hence, computing professionals can act honestly and still not be able to determine all the ethical issues that could arise.

A proposed solution is to combine and leverage multiple techniques in addition to these guidelines such as anticipatory and experimental approaches. These approaches use a combination of qualitative and quantitative measures to evaluate the ethical dilemmas posed by emerging technologies such as conducting future studies, scenario analysis, forecasting, impact assessment, risk assessment, public and stakeholder engagement.

13.1 Anticipatory approach

Anticipatory approaches allow analysis of ethical issues by using various kinds of qualitative and quantitative measures such as Delphi panels, trend analysis, forecasting, future studies, and horizontal scanning. Such techniques allow an organisation to predict and resolve ethical issues before they could arise. Some examples of anticipatory approaches that exists are briefly summarized below:

Techno-Ethical Scenarios Approach: Scenario analysis is used as the basis for this approach. Scenario analysis is a well established technique for anticipating issues that may arise in the future (Brey, 2012). This approach consists of three main steps:

1) **Sketching the moral landscape:** Describe the technology, current ethical standards, practices and regulations.
2) **Generating potential moral controversies:** This is done using the NEST-ethics. It is a taxonomy of past ethical issues that have previously occurred and noted.
3) **Constructing closure by judging plausibility of resolutions:** Multitude of arguments and views are analysed to deduce ethical issues that have the most probability of occurring.

Ethical technology assessment (eTA): This assessment can be conducted by completing a checklist that refers to nine crucial ethical aspects (Palm and Hansson, 2006):

1) Dissemination and use of information
2) Control, influence and power
3) Impact on social contact patterns
4) Privacy
5) Sustainability
6) Human reproduction
7) Gender, minorities and justice
8) International relations
9) Impact on human values

Ethical impact assessment: Based on these core principles (Respect for autonomy, Nonmaleficence (Avoiding harm), Beneficence, Justice, Privacy and data protection). A set of values are proposed under each of these principles and the organization must strive to adhere to these values. For example, the core principle, Privacy and data protection, enshrines the following values: Collection limitation (data minimisation) and retention, data quality, purpose specification, Use limitation, Confidentiality, security and protection of data, transparency, individual participation and access to data, anonymity, privacy of personal communication, privacy of the person and privacy of personal behaviour (Brey, 2012).

13.2 Experimental approach

It is based upon the idea that risks related to emerging technologies cannot be properly quantified. This is because these technologies are new and hence significant research does not exist regarding its consequences. Therefore, experimental approaches relate to introducing a technology as a social experiment first. Several frameworks have been proposed for responsible technology experimentation such as An Ethical Framework for Evaluating Experimental Technology (Martin, 2018).

Conclusion

Various frameworks are being introduced around the world to enact measures related to information privacy. Several such examples were discussed in this paper such as the recent enforcement of GDPR in Europe. The ACM Code of Ethics was also updated for the first time since 1992 to keep up with recent advancement in technologies. Additionally, the COBIT framework also received major updates in 2018. This gives us the view that the era of ‘no privacy’ may only be temporary because governments and organisations are taking major efforts to enact information privacy measures that align with evolving digital technologies. However, current trends show that such legislations are usually implemented after these technologies reach the consumer market. Introduction of such frameworks and legislations must keep up with the pace of technology. Finally, organisations should take a multidimensional approach towards ethical issues posed by emerging technologies. Organisations which operate in jurisdictions that enforce data protection regulations (Example: GDPR in EU, COPPA in California) should strive to adhere to these standards. Organisations which operate in jurisdictions that do not enforce data protection regulations can still strive to be ethical by implementing a combination of approaches such as the ACM Code of Ethics, Anticipatory and Experimental approaches.

References

Acm.org. 2018. *ACM Code of Ethics and Professional Conduct*. [online] Available at: <https://www.acm.org/code-of-ethics> [Accessed 25 May 2021].

Ahmed, S., Haque, M., Chen, J. and Dell, N., 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW), pp.1-20.

Becker, M., 2019. Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. *Ethics and Information Technology*, [online] 21(4), pp.307-317. Available at: <https://link.springer.com/article/10.1007/s10676-019-09508-z>.

Brey, P., 2012. Anticipatory Ethics for Emerging Technologies. *NanoEthics*, [online] 6(1), pp.1-13. Available at: <https://link.springer.com/article/10.1007/s11569-012-0141-7#citeas> [Accessed 29 May 2021].

Federal Trade Commission, 2002. *Children's Online Privacy Protection Act*. [online] Federal Trade Commission. Available at: <https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf> [Accessed 25 May 2021].

Harisaiprasad, K., 2021. *COBIT 2019 and COBIT 5 Comparison*. [online] ISACA. Available at: <https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison> [Accessed 25 May 2021].

Knopp, C., 2019. Privacy Perception in Developing Countries. [online] Available at: <https://www.researchgate.net/publication/337211237_Privacy_Perception_in_Developing_Countries> [Accessed 25 May 2021].

Kramer, A., Guillory, J. and Hancock, J., 2014. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, [online] 111(24), pp.8788-8790. Available at: <https://link.springer.com/article/10.1007/s10676-019-09508-z>.

Martin, D., 2018. Sven Ove Hansson (ed.): The Ethics of Technology. Methods and Approaches. *Ethical Theory and Moral Practice*, 21(5), pp.1247-1249.

Morton, H., Stanton, R., Zuppa, J. and Mehta, K., 2005. Food advertising and broadcasting legislation-a case of system failure?. *Nutrition & Dietetics*, 62(1), pp.26-32.

Palm, E. and Hansson, S., 2006. The case for ethical technology assessment (eTA). *Technological Forecasting and Social Change*, [online] 73(5), pp.543-558. Available at: <https://www.sciencedirect.com/science/article/pii/S004016250500082X?via%3Dihub> [Accessed 29 May 2021].

Rowntree, O., 2018. *The Mobile Gender Gap Report 2018*. [online] GSMA. Available at: <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/04/GSMA_The_Mobile_Gender_Gap_Report_2018_32pp_WEBv7.pdf> [Accessed 25 May 2021].

Samsuri, S., Ismail, Z. and Ahmad, R., 2013. Protecting Personal Medical Information: Asian Perspectives. *International Journal of Computer and Communication Engineering*, pp.468-472.

W. Lee, W., Zankl, W. and Chang, H., 2016. An Ethical Approach to Data Privacy Protection. *ISACA JOURNAL*, [online] 6, p.1. Available at: <https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection> [Accessed 25 May 2021].