International Journal of Scientific Research and Management (IJSRM)
||Volume||10||Issue||06||Pages||LIS-2022-25-33||2022||
Website: www.ijsrm.in ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v10i6.lis01

Information Ownership and Privacy Control in Information Society

Godwin, Lucky Stephen, Nwabugwu, Mgbodichima Jummai

Tekena Tamuno Library, Redeemer's University, Ede,
Osun State, Nigeria
Taslim Elias Library, Nigerian Institute of Advanced Legal Studies, University of Lagos Campus, Lagos State, Nigeria

Abstract
Information ownership and privacy control of information are two inter-related aspects of privacy protection that have emerged as essential areas of study for academics, information scientists, businesses, lawyers, and policymakers with the advance of information technology in the information society. Information ownership and privacy control is an essential area of focus in today's digital world and modern information society where information can so easily be captured, stored, and shared. Multidisciplinary privacy research has been conducted for decades. Yet, information ownership and privacy control remains a complicated subject that still provides fertile ground for further investigation, especially in the modern information society. This paper, therefore, discusses the concept and characteristics of information ownership, information privacy control, and information ownership & privacy control in the information society.

Keywords: Information, Information Ownership, Privacy Control, Information Protection, Information Society

Introduction

Information society is a concept that responds to the expansion and ubiquity of information. Information society has been in use since the 1970s, but has gained popularity and is now widely used in modern society. In information society, the term information age is used to describe its time frame were the major activities of the society is centered around the creation, manipulation, integration, usage and the distribution of information. Information Society is a society characterized by a high level of information intensity in everyday life of most citizens, in most organizations and workplaces; by the use of standard or compatible technology for a wide range of personal, social, educational and business activities, and by the ability to transmit, receive and exchange information rapidly between places irrespective of distance. The information society succeeded the industrial society. Unlike the industrial society where steam power and fossil fuels were distinguishing elements, the defining feature of information society is information (Oxford Reference, 2020).

Information is the lifeblood of any modern information society. It is often referred to as one of the most valuable asset and the key concepts in modern information society. The production, distribution, and use of information are some of the key aspects of modern economic activities. Driven by technological information progress, information has become an asset in its own right. This established an information economy and challenged the law to provide an apt framework suitable to promote the generation, collection, processing, dissemination, control, protection and disposal of information, which enable its distribution and efficient allocation, and deal with the risks inherent in information technology. The major component of such a legal framework should be property rights law, copyright law, and information protection law. However, information as an object of property rights is not limited to intellectual property but may also occur as personality aspects or even tangible property. Accordingly, information as property can be found in the area of intellectual property, personality protection, and other property rights. Legal ownership of such information is established by different subjective rights (Zech, 2015).

Ownership rights and privacy control of information are two inter-related aspects of privacy protection that have emerged as essential areas of study for academics, information scientists, businesses, lawyers, and policymakers with the advance of information technology in the information society. As the extensive use of consumer information has become prevalent in the modern marketplace and the value of the information increases, the issue of information ownership and privacy control is raised (Joinson & Paine, 2007). Hence, this paper focus discussion on information ownership and privacy control in an information society.

Information Ownership in Information Society

Information society is driven by activities that are information related, and these activities include; the creation, distribution, evaluation, manipulation, integration etc. of information using information technologies and related technologies. No matter the nature of activities surrounding the information from the time of its creation to its being discarded; an entity either an individual or a corporate body in the society should be responsible for such information, since information has the driving force that positively or negatively impact on the society. As information takes on an increasingly important economic role in the current information society dispensation, the existing frameworks for information ownership are called upon to provide some form of protection for rights in information.

In practical terms, information ownership rights are frequently asserted, although the nature, scope, and robustness of these rights may be uncertain and contingent. In most cases, claims of ownership are based on copyright law, and information protection law asserted under the laws of confidential information. Copyright law and information protection law, which place individual and organization in control protection of their information, have created a context which has resulted in the concept of information ownership (Scassa, 2018), hence, the need to discuss the concept information ownership in information society.

The term information ownership combines two words, information and ownership. A look at the denotative meaning of the words individually would provide a basis for the interpretation of the term "information ownership from a layman's point of view. Information according to Stands4 Network (2020) is any set of facts, knowledge, news, or advice, whether communicated by others or obtained by personal study and investigation; any datum that reduces uncertainty about the state of any part of the word; intelligence; knowledge derived from reading, observation or instruction". Whitten, Bentley, and Dittman (2001) described information as data that has been refined and organized by processing and purposeful intelligence, while the term ownership was defined by the Cambridge Dictionary (2020) as the fact that you own something or the right of being the owner. This implies that for one to be certified as owner there must be a proof that justify the right of ownership on the individual or entity. From the definition of both terms, information ownership can therefore, be defined as the fact or proof that that one owns information that resulted from data that have been refined and organized by processing and purposeful intelligence or having the right of being regarded as the owner of information.

Information ownership is a relatively new concept in the world of information systems and society. Ownership typically means having a legal right to a piece of property like a house or car. When using this definition, ownership can sometimes be unclear when dealing with a digital property like information and data. Commonly, an information owner is a person or organization with the legal right and ability to create, alter, share, or restrict any piece or set of information. Information owners can assign these functions and responsibilities to other parties, such as assigning information system providers to act on their behalf. These providers host information systems to store and process the information and often have the same capabilities as the owner to edit, share, or restrict information.

Technopedia.com (2020) defined information ownership as the act of having legal rights and complete control over a single piece or set of information or data elements. It defines and provides information about the rightful owner of information assets and the acquisition, use, and distribution policy implemented by the information owner. In other words, information ownership is a matter of policy that tends to establish the entity that has the legal right and complete control over item of information that could be an asset, of value or of importance to a society whose major activities are driven by information.

Information ownership is a domain within computing and information ethics. Arguments for various owners of information are considered. Information ownership is primarily an information governance process that details an individual and organization's legal ownership of information. An information owner can create, edit, modify, share, and restrict access to the information. Information ownership also defines the information owner's ability to assign, share, or surrender all of these privileges to a third party. This concept is generally implemented in medium to large enterprises with vast repositories of centralized or distributed information. The information owner claims the possession and copyrights to such information to ensure their control and ability to take legal action if an internal or external entity illegitimately breaches their ownership. The information ownership issue is essentially a control issue, control of the flow of information, the cost of information, and the value of information.

An information owner is an individual or an organization with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal (Committee on National Security Systems, 2015). U.S. Department of Energy (2012) defined an information owner as an individual or organizational official with statutory, management, or operational authority for specified information and is responsible for establishing the policies and procedures governing the generation, collection, processing, dissemination, and disposal of specified information. In information-sharing environments, the information owner is responsible for establishing the rules for appropriate use and protection of the subject information and retains that responsibility when the information is shared with or provided to other individuals or organizations.

Ownership is mostly associated with properties and items whose facts are tangible to easily identify their ownership. For instance documents can be used to validate the ownership of a property like land, car, personal effects etc. However, information ownership is somehow dicey, because information is quite different from other traditional forms of properties such as land, car and personal effects. There are characteristics of information which differentiate them from other traditional forms of properties that can be legitimately owned. According to Hart (2002), these information characteristics are:

- **Intangibility:** Although information may be instantiated in some tangible forms such as computerized database or hardcopy report, fundamentally information remains intangible. For instance, I might decide to write the address of a potential client in my personal phone book or store them in my tablet. I could as well memorize the address for future use. But still, this action will not change the position of the information as it is essentially tacit in nature, thus, giving information that intangibility characteristics.
- **Non-exclusivity:** Information can be used simultaneously. The use of information by one person does not prevent its use simultaneously by another.
- **Usage tolerance:** Information does not deteriorate through use.

The above characteristics of information that differentiate it from physical objects or items are some of the reasons why it cannot be applied to defining information ownership, this is because it would be impossible to lay claim on something that one cannot place a finger on (intangibility), or exclusively utilize. However, there are certain characteristics that information has in common with properties that can be applied in defining and justifying information ownership. Thus, information can be:

- Information can be discovered. The First Occupancy Theory holds that the initiator of a thing is entitle to it. The first to possess or occupy are often considered the owner of a thing (Becker, 1977).
- Resources and efforts are often committed to the collection and production of information. According to Labour Theory of by John Locke in 1689, the adding of value through the mixing of one's labour with something is what confers ownership (Grunebaum, 1987).
- The value of information depends on to whom and when it is available. The Utility theory can be applied to determine the information owner based on value. That is the ownership of information should be allotted in such a way that it will be of maximum benefit to all parties involved.
- Information can enable activities that would be impossible in their absence
- Information is data refined and organized through processing and purposeful intelligence by people.

From the above similar information characteristics, it can be safe to simply put that the ownership of information is based on the entity who discovered information, expended mix of labour and resources in the

production of information, can influence the value and availability of the information, without which there is no value and purpose of the information in enabling activities.

Characteristics of Information Ownership

The owner of the information processed, stored, or transmitted by Information Technology (IT) and Industrial Control System (ICS) may or may not be the same as the IT and ICS owner. Information owners provide input to IT and ICS owners about the cybersecurity requirements and controls for the systems where the information is processed, stored, or transmitted. However, there are four elements supporting information ownership in information society. Ownership is vested on the complex rights which are exercised to the exclusive of all others (The Fact Factor, 2020). The characteristics of information owners are therefore:

- **Right of possession:** the entity that owns the information has the right to possess it. It does not matter if the information is in their custody. The information might have been stolen, pirated, plagiarized, referenced or submitted for evaluation etc. irrespective of these situation, the owner of the information has right to make claims or remove any restriction that would want to hinder their ownership of that information. In cases where the information owner feels that they are being denied or prevented from enjoying the rights allowed of being the owner, they have the right to institute suits to protect damage to their rights. For instance X, Y and Z are different organizations, X's hasa proprietary software that was separately subscribed to by Y and Z, but the ownership right remain with X. Access to the software is only possible with the different authentication information (covering the period of subscription) given to Y and Z separately. If the subscription given to Z had expired and Y gave Z their authentication information to continue enjoying subscription by proxy, X has the right to revoke the subscription enjoyed by Z and Y especially if there is a binding contractual agreement prohibiting sharing of authentication information with other organization. If Y refuse to comply, X can sue Y to Court of law for contract violation,
- **Right of use and enjoyment:** Information owner has the right to use and enjoy the information as they please, they are under no obligation not to use it, but every other person are under obligation not to use it or access it. However, the owner of the information can be restricted by operational law or agreements such as
    - The owner of the information cannot use it in a way that would hurt others
    - The state officials in pursuance of a warrant issued by a Court of law or for any lawful purpose, have a right to access information owned by someone else.
    - The owner is curtailed by the rights of the encumbrance.
- **Right of disposition:** This implies the right of usage, manipulation, revision, destruction, discarding, or integration of information by the owner. The information owner has the right to make use of the information. The owner has the right to review information for which they have ownership and they have the right to transfer the ownership of such information either by conveyance or by will after death. For instance if foodprocessing company "Y" has information on the recipe for producing a particular fruit drink and decide to sell everything about company "Y" to "Z", they can as well transfer the right of ownership of that recipe to company "Z". With respect to "right of disposition", the owner of the information can be restricted by operational law or agreements such as:
    - The owner of the information cannot use it in a way that would hurt others
    - The state officials in pursuance of a warrant issued by a Court of law or for any lawful purpose, have a right to access information owned by someone else.
    - The owner is curtailed by the rights of the encumbrance.
    - Legal restrictions may hamper the unrestricted disposition of information
    - Information owner may not be allowed to dispose same with a view to evade or delay their creditors.
- **Indeterminate duration:** Characteristically, ownership of information has an indeterminate duration, unlike every other non-owner in possession that has interest that is determinable at a point in time. For instance, the interest of a subscriber comes to an end once the subscription expires, whereas the interest of information resource owner to which a subscriber subscribed does not have a

determined end. The interest of the owner is not even determined by their death. The interest of the owner either descends by rules of inheritance or by conditions of will.

- **Residuary nature:** the residual right of the information vest on the owner, even after, lesser rights such as subscription, lease etc. have been given away. Having determined the expiration of the lesser rights, all original rights are revived for the owner. For instance, a satellite cable television company gave right of view to active subscribers; at this point the subscribers have the right to view, they can complain and seek redress if they are not able view channels covered by their subscription for the period, however, once their subscription expires, they loss the right to seek redress, however, the complete right now vest with satellite cable television company, to reward such subscriber with viewing access or not.

Information Privacy Control

In a modern information society, people desire privacy. Yet, at the same time, people willingly share personal information to obtain services such as health care and insurance and make friends. The concept of information privacy control is a multidisciplinary issue and therefore has a variety of definitions. Concepts such as secrecy, solitude, security, confidentiality, anonymity, liberty, and autonomy, amongst others, are often viewed as part of privacy. Some argue that it can be distinguished and is distinctly separate from these concepts, while others say that it is integral to them (Tavani, 2007). The matter of its definition is also closely related to the issue of whether information privacy control should be seen as a right or merely in terms of one or more interests an individual may have (Tavani, 2008).

Law Insider (2020) defined information privacy control as the administrative, technical, and physical safeguards employed within agencies to protect and ensure the proper handling of personally identifiable information or prevent activities that create a privacy risk. Privacy control has been defined in the privacy literature as an individual's ability to exert influence and autonomy over decisions regarding the disclosure and subsequent use of their personal information, as well as freedom from unsolicited marketing communications (Malhotra et al., 2004). Privacy control is considered by individuals and organizations to be an essential aspect for interacting and sharing their information (Hong and Thong, 2013). Information privacy control (information privacy or information protection) refers to: freedom from unauthorized access to private data; inappropriate use of data; accuracy and completeness when collecting data about a person or persons (corporations included) by technology; availability of data content, and the data subject's legal right to access; ownership and the rights to inspect, update or correct these data.

Information privacy control is also concerned with the costs, if data privacy is breached, and such costs include the so-called hard costs (e.g., financial penalties imposed by regulators, compensation payments in lawsuits such as noncompliance with contractual principles) and the soft costs (e.g., reputational damage, loss of client trust). Though different cultures put different values on privacy or make it impossible to define a stable, universal value, there is broad consensus that privacy does have an intrinsic, core, and social value. Hence, a privacy approach that embraces the law, ethical principles, and societal and environmental concerns is possible despite the complexity of and difficulty in upholding data privacy (Lee, Zankl & Chang, 2016).

Information privacy control is an element of information ownership. It is the right of an individual or organization to have control over personal information. An individual or organization must identify the nature of possible threats to its information systems and establish a set of measures, called authorities, to ensure their security and ensure the privacy and confidentiality of such information. Information privacy control is necessary for the modern information society because of the ubiquity of the technology-driven and information-intensive environment. Technology-driven and information-intensive business operations are typical in contemporary society. The benefits of this trend are that, among other things, the marketplace is more transparent, consumers are better informed, and trade practices are fairer. The downsides include socio-techno risk, which originates with technology and human users (e.g., identity theft, information warfare, phishing scams, cyber terrorism, extortion), and the creation of more opportunities for organized and sophisticated cybercriminals to exploit. This risk results in information protection being propelled to the top of the corporate management agenda. The need for information privacy control is also urgent due to multidirectional demand.

Information privacy control becomes an essential information security function to help develop and implement strategies to ensure that data privacy policies, standards, guidelines, and processes are appropriately enhanced, communicated, and complied with, and effective mitigation measures are implemented. The policies or standards need to be technically efficient, economically/financially sound, legally justifiable, ethically consistent, and socially acceptable, since many of the problems commonly found after implementation and contract signing are of a technical and ethical nature and information security decisions become more complex and challenging. Information privacy control is complicated due to socio-techno risk, a new security concern. This risk occurs with the abuse of technology that is used to store and process information (Lee, Zankl & Chang, 2016).

Information Privacy Control Theories

Floridi (2005) discusses two informational privacy theories. These are the reductionist interpretation and ownership-based interpretation. According to the reductionist interpretation, informational privacy is valuable because it guards against undesirable consequences that may be caused by a breach of privacy. The ownership-based interpretation has the view that each person owns his or her information. The theories are not incompatible but emphasize different aspects of informational privacy. However, Tavani (2008) argues that, though these two theories may be appropriate for privacy in general, they may not be for informational privacy. He suggests that most analyses of issues that affect informational privacy use variations of the restricted access and control theories.

According to the restricted access theory, people have informational privacy when they are able to limit or restrict others from access to information about them. Zones of privacy (specific contexts) need to be established to restrict access. In control theory, personal choice is essential and having privacy is directly linked to having control over information about oneself. According to Tavani and Moor (2001), privacy is fundamentally about protection from intrusion and information gathering by others. Individual control of personal information, on the other hand, is part of the justification of privacy and plays a role in the management of privacy. In the framework, a person has privacy in a particular situation if he or she is protected from intrusion, interference, and information access by others (Tavani, 2007).

Furthermore, the restricted access theory emphasizes the importance of setting up zones that allow individuals to limit the access others have to their information. Like the control theory, it also recognizes the importance of individual control. However, it does not build the concept of control into the definition of privacy. It does require that individuals have full or absolute control over their personal information to have privacy; instead, only limited controls are needed to manage one's privacy. More specifically, the individual has control over choice, consent, and correction: the individual needs to be able to choose situations that offer others the desired level of access. For example, to decide to waive the right to restrict others from accessing certain kinds of information about him or her and the individual needs to be able to access his or her information and correct it if necessary.

Information Ownership and Privacy Control in Information Society

Introna (1997) conducted a study on privacy and the computer: why we need privacy in the information society. The author argues that there is something fundamental in the notion of information privacy and that due to the profoundness of the idea, it merits extraordinary measures of protection and overt support. The author also argues that the notion of information transparency is a useless concept without privacy and that accountability and transparency can only be meaningful if encapsulated in the context of privacy. From philosophical and legal literature, the author concluded that the value of information privacy is the essential context and foundation of human autonomy in social relationships and information society.

Gogus and Saygın (2019) conducted empirical research on privacy perception and information technology utilization of high school students. The study was designed to investigate the perceptions of data privacy and the protection of personal data of high school students who are surrounded by the internet, social media, and technology. The perception of high school students' personal information privacy survey was developed and conducted with 1065 high school students. The study presents five main themes, which are: ownership and utilization of different technologies and password sharing, internet utilization, and perception of privacy, social media utilization, perception of personal privacy on social media, knowledge level, and perception of

personal data conservation and information technology utilization. The finding of the research shows that high school students have a personal information privacy control algorithm. However, persons or institutions outside this algorithm are perceived as a threat to their personal information and are rejected. This research suggests developing practices and techniques to overcome students' concerns about information privacy risks that result from the collection and sharing of personal information.

Zang (2019) researched information privacy, data surveillance, and security to investigate how Australian information privacy, lawfully plays a role in the age of big data and modern information society. With the background of big data, the essay tries to put forward the correlative relationship between the protection of information privacy and the privacy law in Australia. The study also discussed the concepts of information privacy and data surveillance under the background of big data, then highlights the importance of information security in the modern information society. The study further provides awareness for readers and the vital role privacy laws can play in the protection of personal information and emphasizes the importance of a continuous evolution for information privacy law systems in the age of big data and modern information society.

Martin, Gupta, Wingreenand Mills (2015) conducted a study to analyses personal information privacy concerns using Q-Methodology. A conceptual framework is developed based on Westin's theory of Personal Information Privacy (PIP). Concourse theory and Q-methodology was used alongside the literature and the New Zealand Privacy Act 1993 to develop a Q-sort questionnaire. The results indicate that for some, information privacy priorities may be stable across contexts. For others, this differs, suggesting that current views of privacy (e.g., Westin's theory) may need revising for the modern information society.

Janeček (2018) carried out a study on ownership of personal data on the Internet of Things to investigate information ownership and privacy control in the modern information society. The study considers whether, and to what extent, the concept of information ownership can be applied to information privacy control in the context of the Internet of Things in the modern information society. The study was framed around two main approaches shaping all information ownership theories. The study reviewed existing debates relating to four elements supporting information ownership and privacy control, namely, the elements of control, protection, valuation, and allocation. The study concluded by outlining a revised approach to information ownership and privacy control that may serve as a blueprint for future work in the information society.

Conclusion

Individuals and organizations today have more information than they have ever had previously. Advancements in technology play a critical role in generating large volumes of information in the modern information society. Information Society is a society characterized by a high level of information intensity in everyday life of most citizens, in most organizations and workplaces; by the use of standard or compatible technology for a wide range of personal, social, educational and business activities, and by the ability to transmit, receive and exchange information rapidly between places irrespective of distance. The characteristics of information of ownership are pointer to the rights enjoyed by information owners. The paper concluded that information security professionals are in urgent need of useful and pragmatic guidance for developing information privacy protection standards. This is because the information security function in a technology-driven information-intensive environment becomes more complicated due to new risk and information privacy protection. Information security becomes a primary concern to management as information ownership and privacy control infringement occur frequently and attracts extensive coverage in the modern information society.

References

1. Cambridge Dictionary (2020).Ownership. Retrieved from https://dictionary.cambridge.org/dictionary/english/ownership
2. Stands4 Network (2020).Definition of information [Blog post]. Retrieved from https://www.definitions.net/definition/information
3. The Fact Factor (2020) Characteristics of ownership. Retrieved 21 May, 2020 from https://thefactor.com/fast/law/legal_concepts/jurisprudence/characteristics-of- ownership/8896/

4. Cambridge Dictionary (2020).Meaning of ownership. Cambridge University Press. Retrieved from https://dictionary.cambridge.org/dictionary/English/ownership
5. Hart, D. (2002). Ownership as an issue in data and information sharing: philosophically based view. *AJIS*, Special Issue, 23-29
6. Grunebaum, J.O. (1987). Private ownership. Routledge & Kegan Paul
7. Berker, L.C. (1977). Property rights: Philosophic foundations. Routledge & Kegan Paul
8. Whitten, J.L., Bentley, L. D. & Dittman, K.C. (2001). Systems analysis and design methods, 5th ed McGraw-Hill
9. Committee on National Security Systems. (2015). Retrieved from https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf
10. Floridi, L. (2005). The ontological interpretation of informational privacy.*Ethics and Information Technology, 7*(4), 185–200.
11. Gogus, A., &Saygın, Y. (2019). Privacy perception and information technology utilization of high school students. *Heliyon, 5*(5).doi:10.1016/j.heliyon.2019.e01614
12. Introna, L. D. (1997). *Privacy and the Computer:* Why we need privacy in the information society. *Metaphilosophy, 28*(3), 259–275. doi:10.1111/1467-9973.00055
13. It Law Wiki. (2002). Federal Information Security Management Act. Retrieved from https://itlaw.wikia.org/wiki/Federal_Information_Security_Management_Act_of_2002
14. It Law Wiki. (2020). Information owner. Retrieved from https://itlaw.wikia.org/wiki/Information_owner
15. Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer Law & Security Review.* doi:10.1016/j.clsr.2018.04.007.
16. Joinson, A. N., & Paine, C. B. (2007).Self-disclosure, privacy and the internet. In Joinson, A., McKenna, K., Postmes, T. and Reips, U. D. (Eds.), *Oxford Handbook of Internet Psychology* (pp. 237-252). Oxford: Oxford University Press
17. Law Insider.(2020). Definition of privacy control**.**Retrieved from https://www.lawinsider.com/dictionary/privacy-control
18. Lee, W. W., Zankl, W., & Chang, H. (2016).An ethical approach to data Privacy protection. *ISACA Journal, 6.*
19. Martin, G., Gupta, H., Wingreen, S. C., & Mills, A. M. (2015). An analysis of personal information privacy concerns using Q-Methodology. Australasian Conference on Information Systems, Adelaide Australia.
20. Oxford Reference. (2020). Retrieved fromhttps://www.oxfordreference.com/view/10.1093/oi/authority.20110803100003718
21. Scassa, T. (2018).Data ownership. Retrieved fromhttps://www.cigionline.org/sites/default/files/documents/Paper%20no.187_2.pdf
22. Tavani, H. T. (2007). *Ethics and technology: Ethical issues in an age of information and communication technology (2nd ed.).* Hoboken, NJ: John Wiley & Sons.
23. Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38*(1), 1–22.
24. Tavani, H. T. (2008). Informational privacy: Concepts, theories, and controversies. In K. E. Himma& H. T. Tavani (Eds.), *The handbook of information and computer ethics* (pp. 131–164). Hoboken, NJ: John Wiley & Sons.
25. Tavani, H. T., & Moor, J. H. (2001).Privacy protection, control of information, and privacy-enhancing technologies.*ACM SIGCAS Computers and Society, 31*(1), 6–11.
26. Technopedia.com. (2020). Data ownership. Retrieved from https://www.techopedia.com/definition/29059/data-ownership
27. U.S. Department of Energy. (2012). Retrieved from https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf
28. Understanding data ownership. Retrieved from https://www.jbassoc.com/wp-content/uploads/2018/03/3.1-Understanding-Data-Ownership-Data-System-Toolkit.pdf
29. WhatIs.con. (2020).Information society. Retrieved from

https://whatis.techtarget.com/definition/Information-Society
30. Zang, J. (2019). Information privacy, data surveillance and security: How Australian privacy law fully plays its role in the age of big data. *Journal of Educational Theory and Management*, *3*(1), 22-30.
31. Zech, H. (2015). Information as property. Retrieved fromhttps://www.jipitec.eu/issues/jipitec-6-3-2015/4315/zech%206%20(3).pdf

Reference

1. Cambridge Dictionary (2020).Ownership. Retrieved from https://dictionary.cambridge.org/dictionary/english/ownership
2. Stands4 Network (2020).Definition of information [Blog post]. Retrieved from https://www.definitions.net/definition/information
3. The Fact Factor (2020) Characteristics of ownership. Retrieved 21 May, 2020 from https://thefactor.com/fast/law/legal_concepts/jurisprudence/characteristics-of-ownership/8896/