Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 3, 6870-6881
Bareq Muntadher Abdul Wahhab et al.

The Concept of Online Privacy and Personal Data Protection in Iraq: A Way Forward

Bareq Muntadher Abdul Wahhab
Faculty of law, Universiti Kebangsaan Malaysia
(Corresponding Author: bariq_montder@yahoo.com)

Safinaz Mohd Hussein
Faculty of Law, Universiti Kebangsaan Malaysia
(finaz@ukm.edu.my)

Ramalinggam Rajamanickam
Faculty of Law, Universiti Kebangsaan Malaysia
(rama@ukm.edu.my)

ABSTRACT

The growing daily data transmission has exposed individuals to personal data breach and affected their rights to enjoy data privacy and protection online. Although the phenomenon has inspired Iraqi legislators to propose the Information Technology Crimes Bill in 2011, expected to be passed in 2020, inadequate online privacy and data protection awareness in Iraq has prevented the passing of the Bill and created uncertainty on the country's personal data protection. It is vital to understand Iraq's position on data protection to define it as well as online privacy. Hence, the study aims to analyze the sufficiency of personal data protection under existing Iraqi laws to provide such protection and construe definitions of several essential terms. The study employed a doctrinal research methodology which is generally referred to as a library research study. The approach involved analysing the Iraqi Constitution, Iraqi Civil Code 1951, Iraqi Penal Code No. 111 of 1969, academic journals, books, and online databases. The study also highlighted relevant provisions under the Information Technology Crimes Bill and other existing laws connected to data protection under the Iraqi legal system. Resultantly, it was revealed that certain definitions are needed to improve the protection of online privacy and data protection under existing Iraqi laws. In this context, the current study proposed to amend existing laws.

Keywords: online privacy; personal data; data protection; Iraq; Privacy

INTRODUCTION

The rapid growth of technology in the digital century has provided unlimited access to the internet enjoyed by the world population. The swift development of the internet has also increased the collecting and storing of personal data on a large scale. Consequently, the ability to store data on a large scale has exposed Iraqis to a potential breach of data and security risks. One of the measures to protect online privacy and personal data is establishing a set of laws designed specifically for the matter (Mazen, 2015).

Although the idea of a right to privacy has been introduced under the Iraqi Constitution, it is questionable whether the notion is sufficient to protect an individual's online privacy. In

2011, the Iraqi government showed commitment in providing a comprehensive yet controversial law on privacy and data protection by introducing the Information Technology Crime 2011 Bill. Nevertheless, formulating the laws on the right to privacy is not an easy task. Unfortunately, the Bill that should have been passed in 2020 was left unattended. Similar to other laws relating to the citizens' rights and freedom, the Iraqi Constitution only provides general protection for privacy. The constitution does not comprehensively define privacy and whether it includes online privacy and the breach of personal information. Furthermore, no definitive clause was provided to protect Iraqis' fundamental rights. Although the Iraqi Penal Code 1969 provides some provisions regarding the prohibition of disclosing confidential information, the meaning of confidential information remains vague.

Due to the lack of definition under existing laws, the study investigated online privacy and personal data protection in Iraq. Moreover, the concept of a right to privacy and enjoyment of data protection has emerged in Europe under the General Data Protection Regulation (GDPR); hence, the relevant definition under GDPR must be considered to define online privacy and data protection in Iraq. Based on the existing laws in Iraq, the study examined the need to develop the definition for online privacy and data protection in Iraq.

METHODS

The study adopted a doctrinal research method, which is mainly a library research approach. Salter and Mason (2007) explained that the doctrinal research methodology focuses on cases, rules, and principles. These three components involve a substantive content of legal doctrine that is necessary to understand the law. The research method was employed by collecting and analysing the data from primary and secondary sources (Dobinson & Johns, 2007). In the present study, the primary data refers to *the Iraqi Constitution, Iraqi Civil Code 1951, Iraqi Penal Code No. 111 of 1969.* The study also refers to the GDPR as a source for relevant definitions. The definition of specific terms related to online privacy and personal data protection are vital as the GDPR provides a comprehensive set of definitions to provide protection for Iraqis online.

RESULTS

The study results are discussed in the following sections. The results are also divided into sub-categories for a better understanding.

ONLINE PRIVACY AND PERSONAL DATA IN IRAQ

Excess internet usage and personal data proliferation by Iraqi users is overwhelming and persistent. January 2020 alone recorded 29.82 million internet users in Iraq, a 55% (approximately 11 million) increase from 2019. Despite the constant threat to online privacy and personal data, social media users increased approximately 1.9 million between April 2012 and January 2020, with a total of 21 million social media users in January 2020. The figure indicates the amount of personal data exposed daily through various online transaction. Heavy reliance on portable internet devices, smartphones, geographical location devices, smart home facilities, closed-circuit television (CCTV) accompanied with the ability to collect data from such devices have transformed the average life into one whereby personal data is valuable for economic growth (Bo Zhao, 2014).The ill-fitting laws in Iraq create difficulty in

preventing abuses of breach of online privacy and personal data. Generally, the laws should establish fundamental rights that prevent misuse of online privacy with an effective and enforceable remedy towards victims.

An individual's fundamental rights and freedom, particularly the rights to privacy, should be respected and protected at all costs. Hence, it is imperative to comprehend the essential definitions of online privacy, personal data protection, and breach of personal data. Most importantly, there is a need to develop a precise definition for online privacy as one must understand what and when is regarded 'online' to warrant the rights of privacy. The law must also define privacy, whether it only includes privacy to information or extended to personal privacy such as space or tools used online. When a person is online and performs various transactions, the laws must protect their data from being leaked to unauthorised parties from collecting information and abusing the data. Hence, personal data should be precisely defined to accord a person with protection from personal data abuse or hackers. The following sub-headings further examine the definitions of online privacy and personal data under the Iraqi Constitution and GDPR.

DEFINITION OF ONLINE PRIVACY

Privacy has been declared a fundamental right for every human under Article 12 of the Universal Declaration of Human Rights ("UDHR"). Article 12 of the UDHR prohibits any interference with a person's privacy, and everyone is subject to the protection of such interference. In this context, Warren and Brandeis (1890) defined privacy as the right to be left alone. Charles Fried (1990) submitted that privacy is the absence of information and an individual's control over information relating to themselves. In addition, Moor (1997) proposed a different view on Fried's definition of privacy, describing privacy as restricted access instead of having control over personal information. The description is due to the current digital era in which heavy reliance on computer networking makes it almost impossible for a person to control personal information stored in the computer systems worldwide. Hence, he proposed that the best way to protect critical information is to restrict access and only allow authorized persons' access.

Privacy is defined as a person's right to keep their personal matters and relationships secret. On the other hand, privacy is regarded as the quality or state of being apart from company or observation or freedom from un authorized intrusion. Solove (2006) stated that the term privacy is an umbrella term that indicates an extensive and disparate group of related things. Solove also contended that the term privacy is only sufficient for certain purposes, but it should refer to a specific meaning, a view supported by Noura and Karen (2017). Contrarily, Westin (1968) described privacy as the claim of individuals, groups or institutions to determine when, how, and to what extent information about them is communicated to others. Additionally, the right to be alone is the individual's desire for unity, intimacy, concealment, and reservation.

Based on the proposed definition, Westin categorized four states of privacy: 1) solitude- the state of being free from the observation of others; 2) intimacy- a state where seclusion fosters close relationships in a small group; 3) anonymity- when an individual enjoys the freedom from identification and surveillance, and 4) reserve- a state of limited disclosure and the requirement for others to respect that

desire.Nouraand Karen (2017) confirmed Westin's findings in 2004 where people fall into three categories of privacy conception: 1) fundamentalist, 2) pragmatist, and 3) unconcerned. Fundamentalists highlight the accuracy of the collected data, whereas pragmatists tend to disclose certain personal data to a trusted organization. The conceptions differ from the unconcerned, who provides full trust to the organisation to collect their data and believe that it is not considered abusing their rights to privacy (Noura& Karen, 2017).

Although Westin (2003) did not specifically include online privacy in his definition of privacy, Maria and Frank (2008) believed that online privacy should be defined as the traditional concept of privacy. Hence, Maria and Frank (2008) adapted Westin's definition, extending the description of online privacy as "*the claim of an individual to determine what information about himself or herself should be known to others which involves when such information will be obtained and what uses will be made of it by others*."In this context, any information shared online could expose the owner to personal data breach by another person, known as a hacker. Thus, information privacy usually involves the data collected and processed by certain organisations for specific purposes, such as information shared via online purchase or online form.

Summarily, 'online privacy' is the state of seclusion or reservation from others by controlling and limiting disclosure of one's information and controlling how and when the information is communicated when connected to the internet.

PERSONAL DATA

DEFINING PERSONAL DATA

Personal data can be described as an identifier tool such as name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Article 1 (b) of the Organisation for Economic Cooperation and Development's ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013 defined personal data as including any information relating to an identified or identifiable individual (data subject).Personal data is also described as any information associated with an identified person. Eben (2018) stated that 'information' refers to the information related to the individual that makes it directly or indirectly identifiable. Indirect information may include any information which reveals the individual's identity. Hence, personal data is a set of personal information that can be relied on to identify a person.

PERSONAL DATA PROTECTION UNDER GDPR

The European Union (EU) introduced personal data and privacy protection by legislating the GDPR on 25 May 2018. Goncalo, Miguel and Ruben (2019) added that the GDPR lists the responsibility on data storage, data processing, data collection, and data disclosure. The scope of GDPR has prevailed over the previous law, i.e. the European Union 1995 Data Protection Directive (DPD). Under the new regulation, the EU aims to control the use of its citizens' personal data, including empowering their rights, *inter alia,* an organisation must review the process, routines, and procedures when collecting, holding, and processing personal data as per the GDPR. Moreover, the

implementation of GDPR will be supervised by the European Commission to ensure its compliance and conformity.

Article 1 of the GDPR explains the objective of GDPR as a set of rules regarding the protection of a natural person to the processing of personal data, which is recognised as the fundamental rights and freedom of natural persons, particularly the right to privacy of an individual. Article 4 (1) of GDPR further describes personal data as any information associated with an identified or identifiable natural person ('data subject'). An identifiable natural person is a person identified either by direct or indirect identification, specifically by referring to an identifier such as name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

GDPR intends to extend the scope of personal data to include all information connected to an individual. The phrase "any information" indicates that GDPR did not limit the meaning of information, adoptinga wide range of personal data. The term "personal data"also includes any data that provides any information relating to an individual's private life.The phrase "relating to" denotes that the information must relate to an individual. A simple analogy is that the data stored in a smartphone belonging to a person is explicitly connected to that person, and only authorised persons should have access to the said data, as per Moor's restrict access theory introduced in 1997.

The phrase "identified or identifiable" means a person is identified when they are easily distinguished from other members of the group. However, the person who is yet to be identified is referred to as identifiable, meaning they are 'able' to be identified with additional information. Article 4 of the GDPR specified that a person could be identified through identifiers, which include the description of that person, height, skin colour, clothing, and others. The definition also mentions that the person can be identified directly or indirectly. On the one hand, direct identification is the name of the person. However, indirect identification requires a combination of identifiers that describe the person. Hence, Article 4 of the GDPR states the combination of such identifiers precisely.

Article 4 (12) of the GDPR states that a breached personal data indicates that its security has been breached, leading to unlawful destruction or loss or alteration or unauthorised disclosure of data or unauthorised transmission of personal data or storage. Notably, the implementation of GDPR in the European Countries has successfully protected a person's personal data from being breached. The success is due to the obligations enforced under the GDPR that require organisations to comply with the obligations. Non-compliance with the GDPR results in sanctions being imposed by the European Commission.

POSITION IN IRAQ

The current state in Iraq shows no codified law that governs explicitly online privacy and personal data protection. Although the government provides protection, it is regulated under various local legislations, namely the Iraqi Constitution, Iraqi Civil Code 1951, and Iraqi Penal Code No. 111 of 1969.

CONSTITUTION OF THE REPUBLIC OF IRAQ 2005

It is verified that the term privacy is culture-dependent and has different interpretations across various jurisdictions (Bo Zhao, 2014). The right to privacy is embodied under Article 17 of the Republic of Iraq's Constitution, which provides that *"every individual shall have the right to personal privacy so long as it does not contradict the rights of others and public morals".* The clause denotes that every person is entitled to protection from any violation, exposure or interference in private life. Despite the provision, it remains undeveloped and undefined to what extent a person enjoys the rights to personal privacy. The only limitation being as long as it does not contradict other's rights and public morality. Article 40 *"guarantees the right to freedom of communication and all forms of correspondence free from monitoring, wiretapping or disclosure except where necessary for the purpose of security and by court order".* This Article protects individuals from being monitored or spied on daily activities when communicating or corresponding with each other. In this context, they apply equally to the online environment. Hence, it is deduced that people can still enjoy privacy rights when they communicate online, and their personal data is protected under the Iraqi Constitution. With the advancement of the internet of things and technology, these constitutional rights under Article 17 and 40 should be 'upgraded' to adapt to the new reality where privacy means personal privacy that prohibits arbitrary interference, and it should include information privacy (Bo Zhao, 2014).The earlier mentioned data on the use of Internet demonstrates that the daily life of Iraqis has shifted significantly from offline engagement to online engagement, whereby many activities are internet-related activities. The data also indicates that traditional communication has become less efficient among Iraqis, with workre-organised through connected networks that provide real-time data.

The constitutional rights are left unsupported by case laws or other specific laws, which, leaves a vacuum on the definition and application of online privacy and personal data protection in Iraq. Most importantly, privacy protection is deemed a basic need, and Iraqis expect the government to protect their privacy from unwanted interference through codified law.

IRAQI CIVIL CODE 1951

The Iraqi Civil Code describes violations as deviation from one's usual behavior, intentional or unintentional. The deviation includes the intention to harm others or any unintentional conduct which caused harm or injury to another person. Under the Iraqi Civil Code, violations are measured by an objective standard of the usual person. Further, a portion of jurisprudence defined violation of the right to privacy as exposure, interference, arbitrarily, or unlawfully with the privacy of personal data protection. The right to privacy under Iraqi legislation is best defined by describing the breach of the rights as the inviolability of one's home and his confidentiality. It should be noted that the right to privacy comprises two essential elements: secrecy and solitude, also known as seclusion. Thus, everyone has the right to the confidentiality of his private information, correspondence and communication, and respect for his isolation or freedom, including the privacy of personal data protection.

The Iraqi Civil Code 1951 protects an individual's various civil rights, ranging from

the rights to property, ownership, and contractual rights. Nevertheless, it does not explicitly protect the rights to personal information violation or infringement of personal data. It can be observed that the law is disorganised in terms of combining all individual rights under one law. Thus, the law should separate civil rights under specific statutes to ensure exclusive protection instead of using a parent law.

IRAQI PENAL CODE NO. 111 OF 1969

The Iraqi Penal Code provides protection on confidential information. However, confidential information is not defined and it is not clear whether confidential information includes personal data. Paragraph 437 of the Iraqi Penal Code stipulates: any person who, because of his office, profession, trade or the field of his work nature, is privy to confidential information and who discloses such information in the circumstances other than those prescribed by law or uses it to his or another's advantage, is deemed to have committed the disclosure of confidential information. Anyone who committed such an offence may be punishable by a period of detention not exceeding two years and a fine not exceeding 200 dinars or either one. If the disclosure was made with consent or he is authorised to disclose such information, there will be no penalties for such conduct. Furthermore, the law also provides no penalties if he, by such disclosure, intends to report a felony or prevent the commission of such offence.

The following Paragraph 438 of the Iraqi Penal Code specifies types of offences relating to the disclosure of confidential information. Paragraph (1) stipulates that anyone who publishes a picture, remark or information regarding the private life or family life of another, even if such disclosure is true, has committed an offence under the paragraph. Paragraph (2) states that any person other than the person mentioned in Paragraph 328 who is privy to information and discloses the said information to a person other than for whom the information is intended, and such disclosure caused harm to another, has committed an offence under the paragraph. "Any person" under Paragraph 328 refers to the official or employee in a postal telecommunications agency and public official or agent. The paragraph primarily discusses the conduct of the abovementioned parties who open, destroy, or conceal a letter or telex entrusted or consigned to such agency or assisting another person to do the same or reveals the secrets contained therein or contents of a telephone conversation or assist others in committing the same is said to commit the offence under Paragraph 328, punishable with seven years of imprisonment or detention.

Although the Iraqi Penal Code has apparently imposed certain sanctions to ensure its compliance, the lack of a proper definition of confidential information complicates the indictment against a person. In addition, how confidential information is being disseminated, communicated, and disclosed must also be specified to ensure sufficient protection by the law. The specification is crucial to establish the ingredients of the offence for disclosing confidential information. Hence, it could be seen that the Iraqi Penal Code focused on the effect of non-compliance instead of serving the purpose and application of the Act.

INFORMATION TECHNOLOGY CRIMES BILL 2011

The complexity in implementing and protecting the rights to privacy in Iraq is apparent when the Information Technology Crimes Bill 2011 was rejected several times despite its expected approval in 2020. Admittedly, the Bill has loopholes but offers protection for the information shared online and personal data collected through storing user information.

Under Article 1 (12) of the Bill, 'information' includes dates, texts, images, shapes, sounds, codes, database, computer software, and similar elements that create, save, process or send by electronic means. The meaning of "electronic mail (e-mail)"is further elaborated under Paragraph (13), referring to a letter containing information to be created, merged, saved, sent, received completely or partially by electronic, digital, optical, or other similar means.The missing aspects the comprehensive definition of information, which only states that information includes the abovementioned. Thus, it does not explicitly refer to any information connected to an identified natural person, such as identification number, address or images of a person. Additionally, Article 1 did not elaborate on the definition of "electronic means", whether it involves internet connection or computer network or the information communicated via smartphones.

Enacting Article 1 (12) could confuse an individual as 'information' under the provision does not refer to a natural person. Essentially, a natural person refers to a human being. Thus, there is no way that the identifiers such as dates, texts, images, shapes, sounds, codes, a database could mean a natural person or a human being. In principle, personal data can only mean personal information of an identified or identifiable living human. In the context of "living human", the issue is whether the data of a deceased person can be considered personal data. According to Opinion 4/2007 on personal data, the working party agreed that the dead should not be considered natural persons, which does not imply that the data of a dead person cannot receive the same protection. For instance, data of the deceased are kept by medical practitioners who are duty-bound to protect it even after the death of the patient.

One can deduce that the Bill does not intend to protect an individual or a natural person but instead protect the technology stored in a computer or software. Despite the importance of these terms and definitions, the Bill did not address those terms attentively, and it remains vague whether an individual will acquire their right to protection. It could be concluded that the Bill was meant to protect any abuse of technology-related information rather than a person. If the Bill was enforced, Iraq could not claim it as one codified law protecting individuals' rights to privacy and personal data protection when it does not specifically define the scope and application. Therefore, the question is, how can a law protect an individual when they fall outside the definition? Thus, a standard clause is critical to enable the protection and ensure that the said law applies to an individual. It is impossible for a natural person to claim compensation for personal data breach when the law has never included them in the definition.

Chapter 2 of the Bill elaborates on the punishment of various data abuses or information violations. Article 7 (1) of the Bill describes the offence associated with the

intentional use of a computer system or internet belonging to a person, companies, institutions, banks or financial markets and appropriate the property of another person or financial rights or depriving other financial rights through electronic means. The subsequent Paragraph (2) refers to abusing computers or information network to appropriate to himself or others the said software, information, data or codes via an electronic transaction, contract, cards or movable property, deed or signs upon a deed deceptively or impersonating others with the intention to defraud the victim.

Paragraph (3) deals with data tampering, alteration, changing or creating data, statements of account, or software relating to stocks, deed, currency in Iraq or any data, statements of account or software used by any bodiesdealings with stocks in Iraq. Similarly, Article 7 did not refer to the punishment that a person will receive for violating an individual's privacy by disseminating, sharing, and disclosing personal data. Conversely, it lists punishments for individuals who misuse the technology or computer system belonging to other persons or companies. The next paragraph mentions the abuse of computers or information networks deceptively with fraudulent intention. Although Paragraph (2) provides protection by punishing the wrongdoers, the unspecified definition of information and personal data under Article 1 (12) has raised doubt about the effectiveness of the punishment.

Another provision that addresses personal data breach is Article 14 (3) of the Bill. Article 14 (3) stipulates how a person may have committed an offence when entrusted with operating the computers and their control, has intentionally caused damage, disrupt, hinder or defect the computer system or the network. In addition, a person may have committed an offence if he intruded, bothered or called computer or internet users without permission or intentionally logged into a website or information system without permission or used or caused to use the computers belonging to others without permission or unlawfully appropriates telecommunication services via the internet or computers of others. The Article is clear when it involves the restriction on accessing the operation of the computer system, parallel with Moor's theory that states a person can only access the authorised information without abusing such authorization.

The Bill was not drafted explicitly to provide protection against breach of online privacy and personal data; instead, it protects the technology as well as an organization, not an individual. Although information is defined under Article (1) of the Bill, the definition did not specifically refer to a natural person who can either be directly identified or is identifiable through a combination of identifiers. With the growing number of data flows, the Bill is insufficient to combat the riskson the internet. If the Iraqi government intends to consider the Bill, the definition must be drafted comprehensively to grant protection to an individual's online privacy and personal data.

RECOMMENDATION

Several improvements must be made to develop data protection laws and online privacy in Iraq, including proposing amendments to the existing laws to include protection on personal data or developing comprehensive provisions that address the breach of online privacy and data protection. Assuming it is complicated to introduce a codified law to address the right to privacy and

personal data protection, Iraqi legislators should consider introducing an extensive definition of online privacy and personal data under its law to enable such protection.

Based on the aforementioned concepts and descriptions, the following definitions for Iraqi laws are vital:

The following expressions shall have the meanings towards them, for the purposes of the Act:

1) Privacy implies the right to control personal information or the right to own personal information by a person with the aim of being apart from company or observation or freedom from unauthorized intrusion by a third party;
2) Online means controlled or connected to the internet;
3) Computer means each device or group of devices connected with each other that operate automated processing of data;
4) Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person can be identified by referring to an identifier tool such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; for the purpose of the definition, information refers to the information related to the individual that makes it directly or indirectly identifiable. Indirect information refers to any information that will reveal that natural person's identity by combination with other information.[1]
5) Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".[2]

These definitions are mainly derived from the GDPR, which provides comprehensive definitions for the terms privacy, personal data, and personal data breach. These definitions will be useful to develop the effectiveness of personal data protection under existing Iraqi laws. The significance of providing a set of definitions is evident as none of the current laws provided the same. For example, the Iraqi Penal Code only described the sanctions for an offence of disclosing confidential information. However, the term "confidential information" was never defined under the Code. Therefore, a comprehensive definition is required to understand what type of confidential information is covered under the said Code and in what circumstances the information can be disclosed and cannot be disclosed. In the absence of the definition, it is almost impossible for the law to protect an individual's legal right.

CONCLUSION

The increasing use of the internet and computers has exposed many Iraqis to breach of personal data. Hence, effective and elaborate protection must be accorded to them. Although the legislators might initially intend to provide such protection in the existing Iraqi laws, it was formulated insufficiently to handle the threat exposed against such privacy. Hence, Iraqi legislators must seek

[1] Article 4 (1) of Regulation (EU) 2016/679 (General Data Protection Regulation).

[2] Article 4 (12) of Regulation (EU) 2016/679 (General Data Protection Regulation).

another solution instead of relying on the existing laws and unenforceable Bill.

The most noteworthy point from the above proposition is introducing and developing new definition into the current legislation to enable the protection of individual's privacy and personal data. The essence of the definition should grant the Iraqis their constitutional rights as per Article 17 of the Iraqi Constitution. Assuming that the legislators opt to specify the definition under existing laws, it is best to elaborate it under Iraqi Penal Code No. 111 of 1969 as it covers the sanctions for disclosing confidential information. However, the Code does not define essential terms such as personal data to be incorporated with the term confidential information.

The terms "any information", "relating to", "identified or identifiable", and "natural person" should be highlighted to enable protection for individuals under the Iraqi legislation. It is imperative that the term 'information' includes the personal data of a natural person instead of focusing on organisations or technology. The term "personal data" is critical to the extent that it should be interpreted in a wider scope. Broadening the interpretation of the term means any objective or subjective information of a person may fall under personal data irrespective of the medium that holds such data. Moreover, excluding personal data in the definition prevents the law from applying to living human as they fall out of the definition.
The term "relating to" should be defined under the law as it determines the scope of the information. The extension of the meaning is to decide whether the information disclosed or disseminated to other persons is equal to any information relating to a person. Information has multiple meanings, and it can be any information, but most importantly, it must relate to an identified or identifiable natural person. Meanwhile, the term "identified or identifiable" is a condition whereby a person can be identified or considered identifiable through several means; personal data is one way to identify a person.
The existing laws in Iraq can be considered as protecting individuals, but no specific law governs or regulates the dissemination of personal data or online privacy of a "natural person". Therefore, the term should be defined carefully to avoid any ambiguity in the law. The vagueness is apparent in the Information Technology Bill 2011, whereby the definition of information did not include the natural person to enable protection against an individual.

This study proposes that the government develop appropriate guidance and consider the recommendations made above when dealing with online privacy and personal data protection laws. It is important to mention that protection against online privacy and personal data is imperative to gain continuous trust from the public on online transactions and communications. Hence, the study suggests the revision of existing legislation in Iraq and for the proposed definition to be established to ensure that no individual is left out from being protected by the law when they conduct online transactions or communications.

REFERENCES

1. Cambridge dictionary. (n.d.).In dictionary.cambridge.org dictionary. RetrievedJune 21,2021, from https://dictionary.cambridge.org/dictionary/english/privacy
2. Eben, M. (2018). Market definition and free online services: The prospect of personal data as price. *I/S: A*

Journal of Law and Policy for the Information Society, *14*(2),239.

3. Kumar, S. (2022). A quest for sustainium (sustainability Premium): review of sustainable bonds. Academy of Accounting and Financial Studies Journal, Vol. 26, no.2, pp. 1-18
4. Fried, C. (1990). *Privacy: a rational context*. Oxford University Press.
5. Goncalo, A.T., Miguel, M.D.S. & Ruben, P. (2019). The critical success factors of GDPR implementation: A systematic literature review. *Digital Policy, Regulation and Governance*, *21*(4),404.
6. Maria, M & Frank, B. (2008). Online privacy: Measuring individual's concerns.E-Commerce and Web Technologies,5183.
7. Mazen, I.G. (2015). Toward data protection laws and code of conduct in Kurdistan region government. International Journal of Engineering and Computer Science, 4(9), 14149.https://doi.org/10.18535/ijecs/v4i9.14
8. Merriam-Webster dictionary. (n.d.).In Merriam-Webster.com dictionary. Retrieved June 21,2021, from https://www.merriam-webster.com/dictionary/privacy
9. Moor, J.H. (1997). Towards a theory of privacy in the information age. AcmSigcas Computers and Society, 27(3),27-32.https://doi.org/10.1145/270858.270866
10. Noura, A & Karen, R. (2017). Privacy of the internet of things: A systematic literature review. Proceedings of the 50th Hawaii International Conference on System Sciences, 5947. https://doi.org/10.24251/HICSS.2017.717
11. Solove, D.J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 485.
12. Warren, S.D. & Brandeis, L.D. (1890). The right to privacy. Harvard Law Review, 4(5), 193.
13. Westin, A.F. (1968). Privacy and freedom. Washington. & Legal Law Review, 25(1), 166.
14. Westin, A.F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2), 431.