© 2021, Global Media Journal – Arabian Edition Volume 3, Issue 3
ISSN: 2707-6768

Limiting the Social Media's Encroachment into a Person's Right to Privacy

Sagee Geetha Sethu[1], Devika Ramachandran[2]

[1]Amity University Dubai, UAE, ssethu@amityuniversity.ae
[2]Amity University Dubai, UAE, dramachandran@amitydubai.ae

Corresponding Author[*] Sagee Sethu

ABSTRACT: The last decade saw an exponential growth of social media network like Facebook, twitter, linked in and the likes. The social media has made their presence felt in almost every one of our lives and even without realizing, they are slowly encroaching into our private lives. However, this intrusion into our privacy by the social media is not regulated. This study is aimed at analyzing if the already existing privacy laws of a country can be extended to the social media and if so, how effective can this be. This analysis will be based on those regulations of the countries which have successfully extended their privacy laws. The paper will also identify the limitations of such privacy laws when it is made applicable to social media. By having a better understanding the limitations, the regulatory authorities can make effective changes in either the existing laws or make future regulations to curb the adverse impact of the invasion of privacy by the social media.

KEYWORDS: ***social media, right to privacy, legal analysis, online privacy, data protection***

1. Introduction

The greatest challenge that the authors encountered during preparation of this paper is during conceptualizing the concepts of privacy and its deterioration in the social media networks. Every time a co-relation analysis was pursued by the author, ideologies were hit hard by "Privacy Paradox". Privacy paradox is considered to be a phenomenon where the online users mentions their concern about privacy but behaves as if they were not. (Swartz, J., 2000). At every issue that the author entangled had to objectively reconsider the fundamental principle revolving around the privacy paradox ie, if a person is concerned about privacy, then why does he voluntarily open himself to non-private environment. The contemporary concept of right to privacy defies concept of social media and web 2.0. The right to privacy includes "the right to be free from unwarranted publicity, to live a life of seclusion, and to live without unwarranted interference by the public in matters with which the public is not necessarily concerned" (*Strutner v. Dispatch Printing Co.* 1982). It is seen that everyone is engaged constantly in a process of personal adjustment through which a balance of desire to gain privacy along with a desire of an individual to disclose and communicate to third party, in purview of the norms set by the society, depending on both environmental and social conditions. (Westin, 1967) Therefore, post web 2.0 era challenged us to rethink the traditional fundamentals of privacy as a concept and the need for it to be protected would be the greatest challenge in the advent of web 3.0 era.

1.1 The Social Networks and its Impacts

Social networks is a platform by which users create a semi-public profile using web applications. (Boyd and Ellison, 2007). That is, a profile that may have private information of the profile creator can have certain information which are both public as well as private, for communicating with friends, and for building a strong online community. Social networks have brought about a

parallel universe conjunction of public and private worlds. Before social networks, people shared photographs and other private information by sending the physical photographs by post or digital photographs via email. As communication technologies evolved, so too have social networks. Most social networks allow people to upload and share their images and other private identifiable information with multiple people instantly. In some circumstances, people who upload images or current locations on a social network page can identify or 'tag' (Laden, 2014) a third party captured in a photograph or visiting the location. Third parties can upload images of other people without their permission or knowledge.

Another consequence is that personal images that are shared online may be reused and reshared with ease and with inadequate restrictions. Social networking sites receive revenue through targeted advertising (Plummer, Rappaport, Hall, 2007); each advertisement that appears on a person's profile is specific to the information contained in their posts and images. In sharing and exchanging personal images on social networks, there are competing interests that each person has when they share images on social network. The problem here is that people whose images are captured in photographs or the location is tagged and shared online have a limited ability to prevent the misuse of their image or location information. The recent technological advancements has made it easy to capture information, store data, aggregate and redistribute these information and data collected from individual users and can be utilized for various third parties. The individual users are mostly unaware that their data are being stored and utilized, and that these can be quite detrimental to the users, and affect their privacy adversely. (Houghtona and Joinsona, 2010).

1.2 Information in the post Web 2.0

Keeping your information private in the post web 2.0 is no more one's own choice. It's about your friends' choices, too (Bethany, 2017). Web 2.0 was more of social revolution rather than a digital one. Proponents of Web 2.0 therefore reason out that whilst there exist a layer of interactivity, most of the 1990's Web 1.0 applications were generated for mass audiences and it focused only on the 'passive delivery of top-down content', which the broadcasting of the same was from 'one-to-many'. On the contrary, Web 2.0 applications permits users for participating in almost everything, from the beginning stage of creation to refining the contents as well as distributing and sharing these contents directly. For instance, when a person is tagged in an online content automatically other users will be able to sort and share the content with other users at the same time while at the same time appropriate these existing content and re-use them for producing their own content (Beer, D. and Burrows, R. 2007).

The open nature of Web 2.0 application brought with it some major challenges to the traditional notion of enterprise approach that includes control of intellectual property over information that are being shared as well as the surety of the application Web 2.0. Improving the functionality and interactivity of this application has augmented the ways in which such an application can be easily hacked and threatened by virus attacks; thereby posing serious security threats for many organizations. Other risks can also be found, that could lead to hacking, stalking and abuse of personal information, while sharing information with the use of social networking sites (Bin Al-Tameem, A., Chittikala, P. and Pichappan, P. 2008). Like many important concepts, Web 2.0 lacks a tough frontier, yet having a gravitational core (O'Reilly, 2007). As flaccid as the concept is, vulnerabilities of such a digital social ecosystem are enormous and would directly impact the privacy rights of the mankind. It clearly means we need to start thinking about privacy differently. Now we think only about private space. We behave as if we have keys to the rooms and it is upon us to allow people to enter.

Garcia is his article gives a good anecdote to give a better understanding of the social media sharing of information (Garcia, 2017). He says that it is more or less like being covered in a wet paint consisting of our personal information and if we touch anyone else with that paint, it will definitely leave a handprint of your information on that other person. The more you touch other people, more handprints are implanted on those many number of people. Whoever is looking at these people with their paint covered sleeves can easily comprehend the share of your paint, which is basically your personal information. Hence, it can be seen that we have no control over our privacy and this makes it difficult for any person to protect his or her own privacy. Garcia compares it with climate change stating that like climate change matters cannot be solved on your own, one cannot solve his privacy matter on your own when it is shared in the social media. Like climate change, it is either everyone's problem or no one's problem. (Garcia, 2017).

2. Privacy, right to privacy and evolution of Privacy laws

Privacy can be historically traced its origins in philosophical discussions of Aristotle whereby he makes a distinction between two spheres of life. According to him, there is on one hand the public sphere, which is concomitant with political life, and on the other hand is the family and domestic life, forming the private sphere (DeCew, 2018). There was no organized or systematic treaties related to privacy in United States till 1890 and later we can see the development of privacy law in the US. (DeCew, 2015). Many eminent anthropologists including Margaret Mead have explained the ways in which various cultures have protected the privacy through means of concealment or seclusion or by conducting secret ceremonies, thereby restriction access to others (Mead, M., 1949). According to a survey made by Alan Westin (1967) on studies of animals, it was well demonstrated that it is not only the humans place importance to privacy, but the animals too desire privacy (Westin, 1967).

The right of an individual to have his person and property protected was a principle recognized since the origin of common law. However, it became necessary to broaden its definition and contexts as well as the nature of protection and it's extent, from time to time. The changes in the political, social and economic spheres entailed that newer rights were recognized and the law adapted itself to these ever-changing demands of the society. (Warren and Brandeis, 1890). In earlier times, the only remedy available was for the wrong of trespassing, which was particularly against physically interfering with life and property of any individual. During that time, right to life was seen only in the context of the crime of battery and its various form; where as the concept of liberty related to freedom from actual restraint; and an individual's right to property included his land and cattle. Later, there was considerable change from now merely recognizing a person's physical property, but also his spirits, including the feelings and the intellect of man. There was a gradual change in broadening the scope of these legal rights, which led to a wider understanding of right to life which encompass not a mere existence, but to enjoy life in all aspects, including the right to be let alone. The right to liberty now ensures the exercise of all civil liberties and privileges. Furthermore, the concept of property has developed comprising of all forms of tangible as well as intangible property. (Warren and Brandeis, 1890).

The illustrious essay "The Right to Privacy" by Samuel Warren and Louis Brandeis (Warren and Brandeis, 1890), discussed above, has a clear and methodical discussion on the concept of privacy. Citing "political, social, and economic changes" where it establishes "the right to be let alone", the authors argued about the existing law by saying that it is a way to protect each individual's privacy, and the law sought to elaborate the nature and scope of the protection. The growth of the press and publicity then, though allowing new inventions including newspaper and

photographs, had also increased the reference to violations in the contexts of invasion of privacy which is brought about by public dissemination of information relating to the private life of an individual. According to Warren and Brandeis, many of the cases could be considered as falling within a more general privacy right, that would accord protection to the extent to which an individual's emotions, thoughts, and sentiments, are shared with others. They mention that they were not making any effort to safeguard products or intellectual property but said that right to privacy depends on "inviolate personality" principle, which falls within a person's general right of immunity or the "the right to one's personality" (Warren and Brandeis 1890). This principle is believed to be a part of common law whereby the protection of an individual's property is given priority but the invasion of newer technology has moved away from a general right to a more explicit and separate establishment of a specific privacy protection. (DeCew, 2018).

In spite of the protection of privacy accorded under tort law, whereby the individual has recourse to courts for control of one's own information, and the universally accepted concept on informational privacy, it has been argued by philosophers such as Abraham L. Newman (2008), that countries such as United States and many Asian countries have focused on the development of a limited system of privacy protection, which specifically emphasizes on self-regulation in both industry and government spheres where most of the personal information are readily available.

On the contrary, when we look into the EU and certain other countries, they have implemented an alternative system that highlights protection of consumer and privacy of individual against financial interests of organizations and public authorities. Around 27 EU nations have adopted EU's Data Protection Directive that was enacted in 1995. EU privacy protection laws have spread fast across the world but USA stands as a major exception. United States is the one who has transformed and made the global privacy debate, yet they relied on laissez-faire attitude on privacy protection of personal information and came up with some privacy guidelines. Apart from these, legislations such as the Children's Online Protection Act (COPPA, 2000), The Health Insurance Portability and Accountability Act (HIPPA, 2006) of the US regulate privacy aspects relating to student records and video rentals.

3. Global trends in regulating online privacy

In today's technological era data travels across the globe through borderless networks and the importance of regulations on privacy has become prominent. As per January 2021, more than 130 jurisdictions around the world enacted data privacy law. These laws meet minimum formal standards based on International agreements and covers both private as well as public sectors. Around 102 omnibus data privacy law have been enacted outside EEA (European Economic Area) which includes three jurisdictions; China, India and Indonesia with de facto national privacy law and United Arab Emirates (UAE) with omnibus privacy laws that applies to two of the trade zones in the country. There are still many countries to enact privacy law and the bills are on the table. It can also seen that many jurisdictions are trying to strengthen the laws already enacted and Bills are waiting in Parliaments to be passed. Convergence between national data protection laws and various international agreements are being advocated by many policy makers across the globe. Since few years the development of International agreements on the privacy and data protection has increased tremendously. Some of the first implemented International instruments are discussed below.

3.1 The Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data

It is one of the first binding international instrument for protecting a person's right with respect to automatic processing of personal data. The said convention adopted by the Council of Europe, also known as Convention 108 was signed by the member States of Council of Europe in 1981 and came into effect from 1985. In 2018 the convention was modified; and around 35 countries have signed and three countries (Bulgaria, Croatia and Lithuania) have ratified the modified convention. Preamble of the convention emphasizes the need to gain unity and to protect the rights and fundamental freedoms; specifically the right to respect of the privacy, of the citizen of the member countries. (Preamble, Convention No. 108).

One of the main objectives is to secure right to privacy of every individual with regard to automatic processing of personal data relating the person (Article 1). The Convention has covered all basic principles for data protection (Chapter II, Article 4 to 11) and transborder data flows (Chapter III, Article 12). The recently modified convention along with many other things, has also added genetic and biometric data as sensitive data.

3.2 The OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (OECD Guidelines)

Organisation for Economic Co-operation and Development (OECD) plays a prominent role in protecting the respect for privacy since 1980. With changes in the data security system, OECD revised it's old guidelines and in 2013 it implemented the *'Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'*. (OECD Revised Guidelines). The scope of the guidelines mainly applies to the personal data of both public and private sectors in order to reduce the risk to privacy and individual liberties.

In this guideline, it mentions that at the time of collection of data, the purpose for which the personal data is being collects should be specified. (Paragraph 9, Part II. Basic Principles of National Application OECD Guidelines). The guideline also clearly gives provisions on the free flow of date and legitimate restrictions. According to this, without regard to the location of the data, the data controller will be accountable for any personal data under his control (Paragraph 16, Part IV). The guideline of 1980 focused on the legal, administrative and other procedures regarding national implementation. (Paragraph 19 (a) 19 (b)). It recognised the need for extra mechanisms that could promote and protect privacy. The revised guideline approaches in a different way and continue to work that highlights the new digital environment.

3.3 The European Union General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) is considered as one of the toughest and game changer in data privacy and security law around the globe. All the EU member states, the European Free Trade Association (Iceland, Liechtenstein and Norway and Switzerland) (EFTA-country) were following the same pattern and was inspired by Data Protection Directive 1995, a European Union directive, the purpose of which is to regulate the personal data processing and the free movement of these data. Even though there were many data protection laws in EU system, inconsistency and legal uncertainty were increasing. Thus in 2012, European Commission came up with EU data protection reform that included GDPR. It consists of single set of rules, which is applicable across EU. Later in 2016, the European Council established a more stringent regulation, which relates to the protection of natural persons with respect to personal data processing and the free movement of such data (General Data Protection Regulation). As per the previous legislation, personal data included names, addresses and

photographs. Whereas in GDPR, it also extends to IP address and other sensitive personal data like genetic data as well as biometric data. The basic concept of this regulation is to strengthen private fundamental rights in the digital world and it also supports business by giving instructions for companies and other public bodies in the technological market. The provisions of GDPR has specific principles concerning processing of personal data and states that such processing of personal data should follow the fundamental principles of lawfulness, fairness and transparency. (Chapter II Principles, Article 5). It also requires that the controller should provide certain information in the instances of personal data being collected through data subject. (Section 2, Information and Access to personal data, Article 13). Basically, General Data Protection Regulation is based on principles of protection, consent, transparency, and user control. There is also a penal provision, which prescribes fine to the tune of 4% of the annual revenue of a company.

3.4 The Asia-Pacific Economic Cooperation (APEC) Privacy Framework

APEC Privacy Framework was merged with other international instruments in the year 2014 (which was updated in 2015). The major objective of this instrument is to promote a flexible mechanism on privacy and data protection in all 21 APEC member economies. The framework, which is in consistent with OECD's guidelines of 1980, aims to promote E Commerce across the Asia Pacific regions. It has developed to acknowledge the importance of:

a) Protect privacy from the harmful consequences of unwanted intrusions and prevent misuse of individual information,
b) Recognize the free flow of information so as to sustain financial and social development
c) Implement uniform system across APEC member economies to enable global access
d) Advance international mechanisms to develop and enforce information privacy

The framework mainly applies on natural living persons' information and not legal persons. It has been divided into four parts a) Part I- Preamble, b) Part II- Scope & Extent, c) Information Privacy principles and d) Implementation of Privacy framework including guidance to member economies.

Part III includes nine principles that focus on the objective of promoting economic development as well as considering legal and social values. Some of the main principles that are followed by this framework are preventing individual harm, notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, access and corrections, and accountability (APEC Framework, ISBN 981-05-4471-5 (page 11-28)). All Member Economies are instructed to consider certain points that relates to the privacy protection and they are

1) Information sharing among Member Economies (APEC Framework, Guidance for International Implementation, Paragraph 41-43)
2) Cross-border Cooperation in Investigation and Enforcement (Paragraph 44 & 45 - page 35)
3) Cooperative Development of Cross-border Privacy Rules (Paragraph 46-48-page 36)

Table 1: Other Relevant Privacy Laws around the world

Sl.No:	Law Enacted	Year
1	California Consumer Privacy Act (CCPA)USA	Effective from 2020

2	Personal Information Protection and Electronic Document (PIPED) Canada	Effective from 2000
3	Lei Geral de Protecao de Dados Pessoais (LGPD) General Personal Data Protection Law- Brazil	Effective from 2020
4	National Directorate of Personal Data Protection (PDP) Argentina	Finalized in 2017
5	Personal Data Protection Bill 2019(PDP Bill 2019) India	Bill Published in 2019
6	Cyber Security Law- China	Enacted in 2017
7	California Online Privacy Protection Act (CalOPPA) USA	Effective from 2004
8	Bundesdatenschutzgesetz (BDSG) Germany	2010
9	Protection of Personal Information Act (POPI Act) South Africa	2020

4 Data Privacy regulations in Middle East

In certain circumstances, General Protection Data Protection Regulations (GDPR) applies in organizations in Middle East. European Data Protection Board had issued some guidelines that could apply on organizations outside EU. But it is seen that there are many other laws too for few countries of Middle East related to data protection. All the national laws are inspired by the EU's protection principles or GDPR. Since last ten years, Middle East has been flourishing with privacy laws and regulations. In Gulf Cooperation Council (GCC) {Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and UAE} there is no direct general federal law but has enacted data protection laws at national level.

4.1 Bahrain

Personal Data Protection Law (PDPL) was established in Bahrain in the year 2019. Till that there were only general provisions in different laws which covered areas of confidentiality and privacy. Under this law, Personal Data Protection Authority (PDPA) will have the authority to inspect and investigate any type of violations in data protection. Authority also has the power to issue orders to stop violations including emergency orders and fines. The law also gives opportunity for appeals against decisions made by the authority. It specifies on how to transfer of data from Bahrain to any other country according to rules prescribed. There are no particular laws or regulations on online privacy (Data Protection Laws of the World Bahrain)

4.2 Qatar

In 2016, Qatar passed its first data protection law, inspired by EU's data protection principles. It is the first attempt by a GCC member to establish European- Style legislation at the federal level that include collection, use and disclosure of personal data. This new privacy law has many rules and regulations that are applicable to the processing of personal data. It clearly instructs organizations or entities processing individual data to adhere principles of dignity, fairness and transparency. The law has established a separate category relating to ethnic origin, health, children, physical and psychological conditions, religious beliefs, martial relations etc. The major highlights of this law are that it has included provisions on websites targeting children as well as the conditions and restrictions imposed on use of electronic communications for direct marketing. It also provided for violations of any or certain terms of the law which may end up on fine of maximum QAR 5,000,000 (US $1.4 million) (Qatar Personal Data Privacy Law (13) of 2016)

4.3 United Arab Emirates

In United Arab Emirates, the Federal Decree No. 5 of 2012 on Combating Cybercrimes governs the data protection and privacy matters. This decree was further amendment by Federal No. 12 of 2016. Under Article 2 of the federal law, any persons who illegally gain access to information without appropriate authorization or goes beyond the authority prescribed for gaining access; and thereafter unlawfully publishes or re-publishes any data or information is punishable under Article 2 of Federal Law. There are also provisions for unlawful or illegal use of electronic information systems or computer network or any other information related to privacy or disclosure of confidential matters. Under article 21 and 22 such offences are punishable with imprisonment.

A new legislation (Law No. 26 of 2015 on Data Dissemination and Exchange in the Emirate of Dubai) was implemented by Dubai. This new legislation aims in increasing transparency and also to establish the rules of governance related to dissemination and exchange of data. Apart from that there are many other laws that concentrate on privacy law and two financial hubs of UAE; Dubai International Financial Center and Abu Dhabi Global Market and Dubai Health Care City has also come up with specific regulations on privacy. Regulations established by these financial centers are connected with both EU Directives and GDPR (Sethu, 2020)

UAE privacy laws are mainly based on principles on transparency, lawful basis for processing, purpose limitation, proportionality, data minimization, and retention of data. The law also recognizes specific rights such as right of access to actual or copies of data, right to be forgotten, right to error rectification, right of object to processing of data, right to retention, right to object to marketing, and right to complain to the appropriate data protection authority(Chapter 36, The International Comparative Legal Guide to Data Protection 2018). In Article 3 of the Dubai Law, it mention that all the providers of data must make sure that the necessary procedures taken will legally protect the privacy and confidentiality of the customer.

Even Article 379 of UAE Penal Code also carries relevant regulations related to privacy. As per Article 379 of the UAE Penal Code, a person who is entrusted with a 'secret' because of his profession, is prohibited from using or disclosing that secret without the necessary consent of the concerned person. This article permits the use of or any disclosure of the information only with the consent of the party to whom the secret exists. (Sethu, 2020)

Other federal laws that carries provisions related to personal and privacy protection:

i) Constitution of the UAE (Federal law 1 of 1971)

ii) Penal Code (Federal law 3 of 1987)
iii) Cyber Crime Law (Federal law 5 of 2012)
iv) Regulating Telecommunications (Federal Law by Decree 3 of 2003)
v) Stored Value Facilities Regulation (SVF Regulation, 2016)
vi) Information and Communication Technology in Health Field (ICT Health Law, 2018)
vii) Regulation of Data Dissemination and Exchange in the Emirate of Dubai (Dubai Data Law , 2015)

TABLE: 2 Privacy Protection Laws in other Middle East Regions

1	Privacy Protections Regulations (Data Security), 5777-2017 - Israel	May, 2018
2	Law on Protection of Personal Data No: 6698 (PDL)- Turkey	April, 2016
3	E-Transactions and Data Protection Law (Law No. 81 Relating to Electronic Transactions and Personal Data) - Lebanon	October, 2018
4	Data Protection Law- Egypt	July, 2020

5 Conclusion

In conclusion it can be stated that in the past ten years, there have been tremendous increase in the laws enacted exclusive for data protection and privacy. Even though the laws consists of principles including lawfulness, transparency and purpose limitations, it lacks some principles like confidentiality, integrity and data quality. Many countries have put effort to implement new laws or amend the existing one according to the recent growth in usage of social media platforms. Yet, to apply the above said principles and to uphold and protect the privacy, first of all they need to recognize the rights of individuals relating to privacy principles. The paper has tried to throw light on various provisions that could limit the encroachment of social media into private rights. Several laws and regulations have been enacted specifically for data protection and privacy. Still many acts are included as general provision which needs more clarity. One of the important requirement for an effective data protection regime is to set up a uniform system based on uniform principles by all countries across the world. However, it is seen that Middle East has already adopted various effective data security rules for the protection of privacy. The law of UAE, gives amble protection to the users by guaranteeing few of the most important rights relating to privacy, particularly, the right to access to data and get the copies to the data; the right to rectification of errors, if any; the right to be forgotten, if one choses, and also the right to erase one's data.

References

Al-Tameem, A. B., Chittikala, P., & Pichappan, P. (2008, August). A study of AJAX vulnerability in Web 2.0 applications. In 2008 *First International Conference on the Applications of Digital Information and Web Technologies (ICADIWT)* (pp. 63-67). IEEE.

APEC Framework, Guidance for International Implementation

Beer, D., & Burrows, R. (2007). "Sociology and, of and in Web 2.0: Some initial considerations". *Sociological research online*, 12(5), 67-79.

Boyd, D. M. and Ellison, N. B. (2007) "Social Network Sites: Definition, History, and Scholarship," *J. Computer-Mediated Communication* (vol. 13, no. 1, pp. 210–30.)

Brandeis, L., & Warren, S. (1890). "The right to privacy". *Harvard law review*, 4(5), 193-220.

Brookeshire, B. (2017). On social media, privacy is no longer a personal choice. www.sciencenews.org/blog/scicurious/social-media-privacy-no-longer-personal-choice accessed on 20th April 2020

Data Protection Directive, 25 May 2018.

Data Protection Directive, 95/46/EC, October 1995

DeCew, J. "Privacy". *The Stanford Encyclopedia of Philosophy* (Spring 2018 Edition), Edward N. Zalta (ed.), URL = https://plato.stanford.edu/archives/spr2018/entries/privacy/ accessed on 20 April 2021

DeCew, J. (2018). Privacy, The Standford Encyclopedia of Philosophy, Spring 2018 Edition, Edward N. Zalta.

Garcia, D. (2017). Leaking privacy and shadow profiles in online social networks. Science advances, 3(8), e1701172.

Global Legal Group. (2018). *The International Comparative Legal Guide to Data Protection 2018* (5th edition.) Global Legal Group Publication, https://www.bsabh.com/wp-content/uploads/2018/08/ICLG_Data-Protecton_2018_Rima_Nadim.pdf

Houghtona, D. J., & Joinsona, A. N. (2010) "Privacy, Social Network Sites, and Social Relations". *Journal of Technology in Human Services* (vol. 28, pp. 74-94, Issue 1-2)

Ladan, M. I. (2014, August). E-Commerce security issues. In 2014 International Conference on Future Internet of Things and Cloud (pp. 197-201). IEEE.

Mead, M. (1949). Coming of Age in Samoa. New York: New American Library.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD work on privacy https://www.oecd.org/sti/ieconomy/privacy.htm

OECD Revised Guidelines, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79]

O'Reilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & strategies*, (1), 17.

Plummer, J., Rappaport, S. D., Hall, T., & Barocci, R. (2007). The online advertising playbook: Proven strategies and tested tactics from the advertising research foundation. John Wiley & Sons.

Qatar Personal Data Privacy Law (13) of 2016

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Sethu, S. G. (2020, July). Legal Protection for Data Security: a Comparative Analysis of the Laws and Regulations of European Union, US, India and UAE. In 2020 *11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.

Simpson, A.P., & Sotto, L.J. (2020). Data Protection & Privacy 2021. *Law Business Research.* <https://www.huntonak.com/images/content/7/2/v2/72602/2021-GTDT-Data-Protection-Privacy-Hunton-version.pdf>

Strutner v. Dispatch Printing Co., 2 Ohio App. 3d 377 (Ohio Ct. App., Franklin County 1982).

Swartz, J. "'Opting In': A Privacy Paradox", *The Washington Post*, 03 Sep 2000, H.1.

Treaty No.108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (Council of Europe)

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, 25(1), 166.

Westin, A.F. (1967). *Privacy and Freedom*. New York: Athenum. Pp. xvi, 487