LEBANESE AMERICAN UNIVERSITY

Personal Data and Online Marketing: A Legal Analysis

By

Jouana Mohamad Ayoub

A thesis

Submitted in partial fulfillment of the requirements

for the degree of LLM in Business Law

Adnan Kassar School of Business

July 2020

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS APPROVAL FORM

Student Name: Jouana Ayoub I.D. #: 201906093

Thesis Title: Data Protection and Online Marketing: A Legal Analysis

Program: LLM in Business Law

Department:

School: Adnan Kassar School of Business

The undersigned certify that they have examined the final electronic copy of this thesis and approved it in Partial Fulfillment of the requirements for the degree of:

LLM in the major of Business Law

Thesis Advisor's Name: William Melki

Signature: [redacted] Date: / / (Day / Month / Year)

Committee Member's Name: Dr. Khodr Fakih

Signature: [redacted] Date: 14/7/2020 (Day / Month / Year)

Committee Member's Name: Dr. Abbas Tarhini

Signature: [redacted] Date: / / (Day / Month / Year)

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS COPYRIGHT RELEASE FORM

LEBANESE AMERICAN UNIVERSITY NON-EXCLUSIVE DISTRIBUTION LICENSE

By signing and submitting this license, you (the author(s) or copyright owner) grants the Lebanese American University (LAU) the non-exclusive right to reproduce, translate (as defined below), and/or distribute your submission (including the abstract) worldwide in print and electronic formats and in any medium, including but not limited to audio or video. You agree that LAU may, without changing the content, translate the submission to any medium or format for the purpose of preservation. You also agree that LAU may keep more than one copy of this submission for purposes of security, backup and preservation. You represent that the submission is your original work, and that you have the right to grant the rights contained in this license. You also represent that your submission does not, to the best of your knowledge, infringe upon anyone's copyright. If the submission contains material for which you do not hold copyright, you represent that you have obtained the unrestricted permission of the copyright owner to grant LAU the rights required by this license, and that such third-party owned material is clearly identified and acknowledged within the text or content of the submission. IF THE SUBMISSION IS BASED UPON WORK THAT HAS BEEN SPONSORED OR SUPPORTED BY AN AGENCY OR ORGANIZATION OTHER THAN LAU, YOU REPRESENT THAT YOU HAVE FULFILLED ANY RIGHT OF REVIEW OR OTHER OBLIGATIONS REQUIRED BY SUCH CONTRACT OR AGREEMENT. LAU will clearly identify your name(s) as the author(s) or owner(s) of the submission, and will not make any alteration, other than as allowed by this license, to your submission.

Name:

Signature: [redacted]

Date: 16 / 07 / 2020
Day Month Year

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

PLAGIARISM POLICY COMPLIANCE STATEMENT

I certify that:

1. I have read and understood LAU's Plagiarism Policy.
2. I understand that failure to comply with this Policy can lead to academic and disciplinary actions against me.
3. This work is substantially my own, and to the extent that any part of this work is not my own I have indicated that by acknowledging its sources.

Name:

Signature: 

Date: 16 / 07 / 2020
Day Month Year

DEDICATION

To my father, mother, brother, and sister. Without the support of each and every one of you, I couldn’t have made it here.

To you, I dedicate all my work, hoping that I will make you proud.

ACKNOWLEDGEMENT

Big thanks to the honorable committee including Dr. Khodr Fakih and Dr. Abbas Tarhini for their time and cooperation, and my advisor Attorney William Melki for his constant guidance and support.

Finally, I would like to thank LAU for giving me this opportunity, and its dedicated staff for always being available to provide the needed help and assistance.

Personal Data and Online Marketing: A Legal Analysis

Jouana Mohamad Ayoub

ABSTRACT

Advertisements following users from one screen to another have become common nowadays. Companies process users' personal data to target users and create personalized advertisements, the thing that raises concerns about the privacy of personal information. This has triggered the enactment of regulations that cover data protection and processing for advertising and commercial purposes.

In this research, we study the GDPR, which is considered the world's standard regulation of data protection, and similar laws from UK and the US. In addition, we evaluate the current E-Transactions law and Consumer Protection Law in Lebanon.

We identify the factors effecting the regulatory activity and the risks imposed by data processing. An approach to Amazon's activity is studied, and finally we suggest multiple recommendations to ensure the best practice and safety of users.

Keywords: Privacy, Personal, Data, Regulations, Targeted Advertising, Personalized Advertising.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

GDPR: The General Data Protection Regulation

GDR: General Data Regulation

PECR: Privacy and Electronic Communication Regulation

DPA 2018: UK Data Protection Act

CCPA: The California Consumer Privacy Act

SAR: Subject Access Request

DPO: Data Protection Officer

EDPB: European Data Protection Board

ICO: Information Commissioner's Office

TCF: Transparency and Consent Framework

CMP: Consent Management Platform

IAB: Interactive Advertising Bureau

EEA: European Economic Area

SME: Small to Medium sized Enterprise

ICC: International Chamber of Commerce

CIA: Central Intelligence Agency

Chapter One

Introduction

There is no doubt that numerous businesses have emerged all over the world throughout the past decade. The internet has had an impartial role in the evolution of small to medium sized enterprises into multi-national corporations.

Online trade and marketing is constantly emerging, from online shopping, social media platforms, to targeted and personalized advertisements. Today, almost the smallest piece of information in any conversation could be used to promote goods and services. For example, any two people could be having a conversation about the summer season, when beach resort deals and pool supply ads pop on their screens.

The confusion in such situations is very common, as we are always left wondering: How is this possible? How are companies capable of guessing what we might be interested in? Is this even legalized? To what extent are personalized advertisements regulated? If companies can get customer data from a click, then what are the limitations to such exposure? And what are the laws protecting persons and regulating online marketing? And the list of assumptions and questions goes on and on.

In an interview with 4 News Chanel, Professor Shushana Zuboff said that: “97% of facebook’s revenues comes from its online targeted advertisements.” (Zuboff) This fact highlights the reality that personal data has become the greatest asset nowadays.

Just as facebook, many companies have achieved very high revenues and become the wealthiest in history. This has triggered the necessity of implementing a proper and

updated legal framework for advertisement and trade activity, taking into consideration the different factors that may affect regulations whether politics, governments, or social and economic systems on national, regional, and international levels.

This research aims at studying different regulations governing online marketing with a comparable study to the laws in Lebanon, the factors affecting regulatory activity, the risks imposed by targeted marketing on personal data, and suggestions on this concern.

Chapter Two

Data Protection Regulations

2.1. Background and Impacting Factors:

The regulatory activity is affected by several factors as follows:

2.1.1. The System of the Country:

Each country's principles shape its political, social, and economic system. The regulatory activity and policy implementation are directly affected by the country's fundamental rules.

In liberal countries, where Capitalism is usually adopted, private investments and competition are encouraged. In similar countries, governments usually tend to pass laws that support businesses. While companies view data protection laws as a threat that would restrict their operations, especially when it comes to targeted advertisements using processed user data, they put all their lobbying efforts to fight against data protection laws.

On the other hand, in conservative countries, governments often have control over the economy and are in charge of manufacturing, production, and trade. In those countries, governments might impose limitations on private investments and business growth; however, they do their best to implement policies that enable them to have access to their residents' information to remain in control.

The incentives behind data collection might vary from one country to another, and the entities or purposes that might negatively influence regulating data collection and targeted advertisement are not to be underestimated. However, raising awareness across

societies to the risks of data exposure and learning about people's civil rights is capable of creating sufficient pressure to implement the proper laws.

2.1.2. Business and Corporate Control:

2.1.2.1. Creating Pressure:

As businesses grow bigger and bigger, their power is growing in parallel. Not only does a company's increase in annual revenue and profit help it gain control over the market, but it will plan on expanding in space, equipment, and employment. This will lead to an increase in investment of real estate, manufacturing activities, in addition to the export and import operations.

Hence, when a company has such impact on multiple economic sectors and contributes positively to the economic cycle, regulators will have to think carefully about implementing regulations that would limit its activity.

Today, advertising revenues cover a main part of the annual revenues of the wealthiest companies, like Google, Facebook, or Amazon. Those companies use users' information to determine their preferences and target them in their advertising activity. Amazon, for example, had a total number of almost 800,000 employees in 2019, knowing that this number had been increasing continuously over the preceding 4 years.(macrotrends) The provided high numbers allow these companies to exercise pressure over regulators by threatening to terminate employment contracts if regulations that they believe would limit their activities were passed.

2.1.2.2. Political Endorsement:

Corporations and businesses often engage in the endorsements of political parties or individuals prior to elections. Such endorsements are primarily based on the endorser's

fundamental principles that support one party over another. However, this does not deny that corporations also seek support and facilities that politicians can ensure.

Businesses might classify campaign funding as investments because the elected candidates are the future legislators and they will shape the country's legal orientation. Politicians surely give serious attention to their endorsers' interests by opening doors to public and private partnerships, loosening tax regulations, and other supporting business activities.

Therefore, this motivates businesses to engage in campaign funding and political endorsements, as it will allow them to gain control (Richter).

The Federal Election Commission (FEC) in the US requires that amounts paid for direct advocacy of a specified candidate that exceed $2000 per election, shall be reported. It also requires reporting details about endorsements other than the paid amount, such as who is supported and the type of communication (Commission). The FEC is responsible of monitoring the election campaigns to ensure that candidates are complying with limitations to amounts, taxes, and expenditures to ensure a fair and transparent process. The conditions and limitations to funding and campaign spending vary from state elections to national elections, and according to the type of elections taking place (fec.gov).

In 2016, the spending limit for publicly funding the general elections presidential candidates reached $96.14 million. (T. F. Commission)

In Lebanon, the Supervisory Commission over the electoral campaigns is responsible of overseeing the compliance of candidates and media with competition rules, and it is also the supervisory authority over the electoral spending [elections.gov.lb].

However, in Lebanon the problem lies within the proper enforcement of rules, especially when cabinet members are allowed to run for the parliament.

In the 2018 elections, the Prime Minister, the Minister of Foreign Affairs, and the Minister of Interior and Municipalities (transparency.org) all ran for parliamentary elections while being part of the executive authority in charge of the elections (Jen Pollakusky). This poses direct and clear conflict of interest, making it impossible to perform appropriate supervision, and resulting in high risk of violating the set spending ceilings. As a result, corporations are encouraged to spend more on political endorsements, even if part of the paid amounts is used to illegally gain voters or to for the personal profit of the candidates.

Therefore, other than the possibility of involvement of politicians in businesses, political endorsements might be used by corporations to control future legislators.

2.1.2.3. Participation of Parliament Members in Commercial Activity:

While parliament members are expected to be full-time community servers, it is very common for them to be businessmen, intermediaries, or shareholders in companies. Even though they might essentially have professions related to law, medicine, engineering or other fields, often when they engage in politics they get exposed to what they might consider “opportunities” to benefit from the government’s treasury, while they are in fact taking over public assets. Thus, politicians might advocate for certain projects or partnerships with private companies that they might be partners in, or might be achieving profit for serving their interests.

The majority of Lebanese politicians are known for having their wealth multiply after taking over governmental positions. This behavior raises the concern that, in Lebanon at

least, politicians would put their efforts to pass legislations that serve their private interests rather than the public, and at the same time disregard the enforcement of well-developed legal frameworks that can keep up with current regulations because this might limit their commercial activity or financial resources.

2.1.2.4. Regulatory Entrepreneurship:

Regulatory entrepreneurship is when profit seeking entities choose to build businesses knowing that the law might be against them, but they work on changing the law to be in their favor. Those companies plan on changing the law from the beginning, and often expand and "grow too big to ban" as a way of securing large numbers of consumers that could be influenced (BARRY).

This policy is often adopted in relatively new business sectors, most likely related to technology, because their regulations might be ambiguous, unclear, or unfavorable. In this case, regulatory entrepreneurs will work on shaping the law in their favor to prevent laws that might restrict their activity.

Uber is a very popular example of Regulatory entrepreneurs, where the taxi cab industry in US states requires the possession of a special license issued by the government. The company built its success through connecting people with drivers based on supply and demand, and without having a license for itself. Uber grew bigger and bigger by making offers, which helped it secure a large user base when faced with resistance in New York City. Users were influenced by it and eventually voted against proposals that were intended to restrict its activity (BARRY).

Regulatory entrepreneurship could also be adopted by online advertisers that already have access to user data. They might use the profiles built to determine their interests,

target them with personalized advertisements to gain their support and loyalty, and eventually influence them to vote with laws that the company had been planning. Those companies might view privacy regulations as limitations to their activity or might target the audience to vote with the laws that suit them.

2.2. The Regulatory Framework:

2.2.1. The GDPR:

The General Data Protection Regulation, passed by the European Commission in 2018, is considered a quantum leap in data protection. Article 4 of the Regulation defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a 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."

2.2.1.1. Scope:

This law is intended to cover EU Member States and the European Economic Area, to ensure harmonization of regulation within the region. It applies to personal data, individuals, organizations and companies that include both controllers and processors in the EU. It also applies to businesses based outside the EU, but that work in the EU or are controllers of EU citizens, or dealing with the personal data of EU residents.

The law focuses on the protection of natural persons' data in the EU and the EEA from legal entities with economic activity, whether they are located in the EEA or outside,

but engaging in the processing of personal information related to individuals who are residents of the EEA.

Under the GDPR, processing is defined as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

The GDPR assigns the data controllers or processors acting on behalf of controllers to implement the necessary technical and organizational safeguards, and adherence of appropriate data protection policies and approved codes of conduct or certification mechanisms. The law is therefore applicable to both controllers and processors with stricter provisions on the controllers that are responsible of control over the processing personal data, whereas the processors abide by the controllers’ instructions.

2.2.1.2. Rights and Obligations established by the GDPR:

This regulation mainly focuses on maximizing and ensuring the data subjects’ privacy by establishing 7 principles under Article 5, as follows: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

Accountability is the new principle introduced by this law.

The data subject has the right to have access to his/her processed information, to rectification of inaccurate personal data, erasure, restrict processing, data portability,

objection, and automated decision-making and processing. Therefore, he/she has the right to submit a "Subject Access Request" (SAR), free of charge, not subject to a specific format or directed to a specific person in the entity. The processing entities are required to answer the request about the processed information in detail, in addition to the purpose behind processing it and the duration of storing it. This request shall be answered within one month, or else the data subject may complain to the competent supervisory authority in the Member State. Enterprises with more than 250 employees are required to keep such records regardless of whether there is a request by the data subject, as provided by Article 30 of the GDPR.

Large companies processing a lot of sensitive personal data shall appoint a Data Protection Officer (DPO). The DPO shall also be appointed in governmental bodies. The DPO's job is to ensure compliance of the private entities or governmental bodies with the provisions of the GDPR. Controllers located outside the EU, but bound to this regulation, shall appoint a representative in the Union.

Article (7) gives the data subject the right to withdraw his/her consent at any time without affecting the lawfulness of the consent given before withdrawal. Knowing that consent shall be freely given, a contract shall not be conditioned on the consent to process personal data not necessary for performance. Furthermore, the data subject is given the right to request correction of inaccurate processed information, and the rights to objection or erasure related of processed data related to him/her.

Recital (70) of the GDPR establishes the data subject's right to object to data processing when it is for direct marketing purposes, at any time, whether it is limited to initial

processing or will be subject to further processing. This right shall be made clear to the data subject.

Under Article 6 of the GDPR, legal entities are not allowed to process personal data except for a legitimate basis; that could be upon the data subject's consent, for the performance of a contract, for compliance with a legal obligation, for protecting the data subject or other natural person's vital interests, for carrying out a task of public interest or the exercise of an official authority, or for the purposes of legitimate interests pursued by the controller or third party, but taking into consideration the fundamental rights and freedoms of the data subject.

Recital (47) of the GDPR provides that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

The GDPR also protects data subjects from 3rd countries, outside the EU, or the EU and EU Members from data processing or collection through judicial orders or security related requests from governmental bodies.

2.2.1.3. The Consent Requirement:

Article 7 of the law provides the conditions of the consent for processing personal data. The consent shall be provided explicitly and clearly, and it should be easily accessible. The data subject also has the right to withdraw his/her consent even after giving it, and this shall be easily made possible.

The consent needed for processing personal data shall be informed, because the data subject has the right to be aware of the purpose of data collection, usage, storage, and communication with 3rd parties, thus ensuring transparency of communication.

Recital (58) provides that the principle of transparency could be in electronic form, particularly in situations where it is difficult technologically for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. The GDPR also provides that the processing of personal data shall be limited to the minimum necessary purposes.

2.2.1.4. Restrictions:

Article 23 restricts the rights given to data subjects for the purposes of safeguarding national security defense, public security, handling criminal offenses or execution of criminal penalties, general public interest of the Union Member State, protection of judicial independence and proceedings, handling breaches of ethics of regulated professions, protection of data subject or rights of others, and enforcement of civil law claims.

Therefore, the GDPR provisions do not apply in case of:

-Matters of national security,

-Data collection or processing for the purpose of statistical or historical study or research,

-Data collection or processing of the information of a deceased under the national law of a member state,

-A special law governing an employer-employee relationship, or

-Processing for a purely personal or domestic activity by the concerned person, not for economic purposes.

2.2.1.5. The Establishment of Supervisory Authorities:

Articles 54 to 67 acknowledge the establishment of independent supervisory authorities in each Member State to ensure the proper enforcement of the safeguards provided in this regulation. Those authorities shall also receive complains and sanction administrative offenses.

If the same legal entity has several establishments in the EU, then it will be subject to a main supervisory authority in the State of its main establishment for processing activities.

The supervisory authorities of the EU Member States shall cooperate with each other across the Union. Thus, this regulation provides for the establishment of the "European Data Protection Board" (EDPB) as the body responsible for the coordination between all the supervisory authorities across the Union (Articles 68 to 76).

2.2.1.6. Breaches:

Under Article 33, the competent supervisory authority shall be notified of a personal data breach, holding risk on the rights and freedoms of natural persons, without delay, and within 72 hours after becoming aware of it. If there is a delay in reporting the breach, there should be justification.

The breach notification shall explain its nature, the identification of the concerned data subject and their personal data, the consequences of the breach, and the measures taken to manage such breach and mitigate adverse effects.

Breaches have to be communicated to the data subjects as well with clear explanation of its nature and the measures taken. Under Article (82) of the GDPR, the data subject has the right to compensation for the damage caused by processors or controllers in breach of the law provisions.

In case of violation, companies in breach are subject to a fine of a maximum of 20 million euros or reaching up to 4% of the previous year's global annual turnover, according to the highest amount.

Fining violating companies is usually accompanied with lengthy investigations, and might end up in court. However, even if the process resulted in clearing the company's name from accusation, it usually has a negative impact on the company's activity, and could lead to its failure or bankruptcy for ruining its reputation.

2.2.1.7. Implementation:

Ever since passing the GDPR, companies bound to it have started introducing privacy policies to their websites to ensure compliance with the law.

Knowing that the online activity is not limited to a specific region, most companies have been working on the implementation of the GDPR internationally.

Being passed in 2018, this year companies and websites shall be prepared to adopt the GDPR and implement it.

The GDPR is considered as the standard law for protecting personal data from companies performing economic activities and regulation of digital advertising.

2.2.2. The New ePrivacy Regulation:

2.2.2.1. What it is:

In January 2017, a new EU ePrivacy Regulation proposal was published. This proposal aims to replace the ePrivacy Directive as it constitutes an enforceable regulation from the date of its adoption.

The ePrivacy Regulation is intended to achieve consistency with the existing privacy provisions established in the GDPR, and deals with matters more specifically than the GDPR, making it a ‘lex specialis’ with respect to the GDPR.

It addresses privacy of electronic communication data, whether personal or non-personal, and provides protection that would not be limited to natural persons, but extends to legal persons in general.

The proposal also covers targeted advertising and entities working outside the EU, but having direct marketing activities communicated with people in the EU, in addition to providers of electronic communication services to users located in the EU. The scope of protection covers all current and future means of communication and services.

The introduction text of the proposal states that: “Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication, including when the information has been sent, from where, to whom, is not to be revealed to anyone other than to the parties involved in a communication. The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, e-mail, internet phone calls and personal messaging provided through social media.”

This draft emphasizes the importance of confidentiality of electronic communications and protection of all communicated data. Therefore, consent is always required to be clear, affirmative, and stipulated in an agreement to processing, and not an implied consent.

Users shall have the opportunity to choose between different options of data collection, usage, and communication to 3rd parties, rather than only having the option to "Accept all Cookies" as is currently, or to face cookie walls that prevent the users from online services.

This law also addresses direct marketing, email marketing, and marketing callers. The latter would be required to identify their phone numbers or use a prefix to indicate that they are marketers.

2.2.2.2. Implementation:

The regulation was first meant to be passed at the same date with the GDPR, but it is still under discussion.

Even though on October 19th 2017, the European Parliament Committee on Civil Liberties, Justice and Home Affairs (i-scoop.eu), known as the LIBE Committee, voted on the Lariston report on the Regulation (i-scoop.eu) which is a report including amendments to it, the European Council did not pass the regulation yet. (Lesley Sutton)

Lobbying groups, including advertising companies, have been putting all efforts to prevent the enactment of this law, they consider it a threat to their business activities that will result in the impediment of the digital economy.

This draft has not yet been passed and adopted in national laws due to differences in opinion between Member States, which makes its fate unclear for the time being. However, this proposal brings attention to seriousness of the matter of data privacy and protection.

2.2.3. The United Kingdom and Brexit:

2.2.3.1. The Governing Regulations:

In the UK, data processing is regulated in the GDR and the "Privacy and Electronic Communications Directive" of 2003 (PECR).

The PECR applies to cookies and similar technologies related to data processing and usage, whether personal or not. It requires consent as a prior condition to data processing and use, unless strictly necessary to fulfill a function requested by the user. The requirement of informed consent under the PECR aligns with the provisions of the GDPR, where the first refers to the definition of consent in the GDPR.

The user shall be aware of the purposes of storage and usage of the data clearly, and has the right to withdraw his/her consent at any time. In addition, companies and organizations are required to demonstrate that the user has agreed to give a valid consent.

2.2.3.2. The Information Commissioner's Office (ICO):

The ICO is the body in charge of data protection and privacy regulation in the UK.

UK established data controllers and processors, and entities outside the EU processing data of UK residents fall within its scope. The ICO shall be notified of any data breach within 72 hours after recognizing the breach, similar to the GDPR provisions. It is also responsible of deciding fines in case of breach, which could reach up to 500,000 pounds sterling.

2.2.3.3. The Transparency and Consent Framework (TCF):

The Transparency and Consent Framework is a framework established by entities that fall under the GDPR and ePrivacy Directive scope in order to ensure compliance with (Gutwirth) their provisions.

TCF helps businesses engaged in online advertising to explain the details of processing to data subjects, like identifying the stored information, the purpose and legal basis behind storage or processing, third parties involved, and all the details related to the data subject. As a result, consumers will become aware of all the details and capable of deciding whether to give their informed consent or not.

Third party companies might also register with the TCF to help then gain an informed consent in compliance with the GDPR for processing data. Companies may seek assistance from Consent Management Platforms (CMP), which are companies specialized in helping with consent establishment. Such developed frameworks support the advertising industry while complying with the GDPR and ePrivacy terms and conditions.

2.2.3.4. Brexit and GDPR Application:

Upon passing the GDPR of EU in 2018, the UK DPA of 2018 was set for the application of the GDPR in the UK alongside with the country's national laws. Now, the main concern is the implementation of the GDPR upon Brexit.

According to the ICO statement on data protection and Brexit implementation, the GDPR is going to be applicable in the UK without having to appoint EU representatives for UK companies or organizations which have operations directed towards people

located in the EU throughout the transition period of the UK from the Union. (BURGESS)

Since informed consent is a requirement, the previously acknowledged principles in the PECR are no longer in parallel with the GDPR. Those principles are: consent without sufficient details, navigational consent, or not providing information about 3rd parties having access to the data. (UK)

2.2.4. The United States of America: California Consumer Privacy Act (CCPA):

2.2.4.1. Overview:

In USA, each States has its statutes and case law, in addition to the Federal law of the nation that establishes the constitution and fundamental principles, including the regulation of cross-state commerce.

In New York, although the "Shield Act" exists to block data breaches, the privacy act introduced to regulate personal data processing has not yet been successful.

In this research, we will study the California Consumer Privacy Act being a new law in the biggest State in the US with the world's fifth largest economy.

2.2.4.2. Scope of Application:

The CCPA was enacted in 2018, but came into effect by January 1st, 2020. This law aims at achieving protection of the constitutional right of privacy of California State residents with access from California IP addresses. Therefore, the Act applies to California residents, data companies operating in the state, or data companies operating outside the state but providing services to people in the State.

The law applies to:

-companies that operate in California and make $25 million of annual revenue,

-companies that gather data on more than 50,000 users,

-or companies that make ½ or more of its money from user data.

It also applies to persons having businesses in California that do not meet any of the previous cases, but agree to comply with the CCPA voluntarily.

2.2.4.3. Established Rights and Obligations:

The enactment of this law is considered to be motivated by the GDPR in Europe with many companies in the US having already adopted policies complying with the GDPR, because they either have EU users or operate in the EU.

The newly passed law provides consumer rights upon collecting or using their personal data:

Under Section 3, Consumers shall be informed in detail of the party dealing with their data, and to have access and control over their personal information. They shall also be able to request correction or deletion of their collected information, with businesses being held accountable and subject to penalty in case of violation.

Consumers have to be informed of the possibility of using their sensitive personal information for advertising and marketing purposes according to section 3.B.4 of the CCPA.

Consumers also shall be able to opt out of using their sensitive information for advertising purposes. They might also choose to reject communicating their data with

3rd parties that might combine the consumers' information from different sources to create consumer profiles and eventually use it for targeted personalized advertisements.

Businesses on the other hand are required to inform consumers of their activity and the latter's ability to exercise their rights without penalizing them, in a clear and unambiguous way (Norris). However, these business obligations shall not restrict their compliance and cooperation with governmental authorities and orders.

Similar to the GDPR, the CCPA provides that data collection and usage shall be limited to achieve the necessary purposes, and that businesses shall take all appropriate measures for the protection of consumers' personal information.

As for children, their personal information should not be used for incompatible reasons without specific legitimate purposes, or else the business will be liable and face higher penalties.

2.2.4.4. Breaches:

In case of breach of provisions of this regulation, section 15 gives consumers the right to take civil action against breaching entities in order to recover damage, reaching an amount of $750 per consumer per incident, or actual damages, whichever is greater. This number is prone to accelerated multiplication.

The very high amounts that companies might be at risk of paying create an incentive for them to adopt policies complying with the CCPA, even before releasing the law's enforcement regulations.

CCPA breaches could be committed by not informing consumers of their rights, not enabling disclosure requests, refusing to provide consumers with services or putting different prices if they exercise their rights, or charging consumers for exercising their right. Charging consumers for exercising their rights is possible if it was a reasonable fee for repetitive requests.

Other breaches might be misinforming consumers of their data, not updating policies, not answering consumer requests, or answering after the 45-day duration reaching a maximum of 90 days in total when extension is necessary.

If a consumer becomes aware of the breach, he/she shall notify the business of the breach in order to correct it within 30 days. Furthermore, if the business does not deal with the breach in the assigned duration, the consumer can take legal action and the Attorney General would notify the business of it.

If the business is notified of the violation and does not take action, the Attorney General may take civil action and impose a fine of $2500 per breach, and if the violation is international then the fine might reach $7500 per violation.

For now, political parties of the US are still discussing certain implementation issues for the enforcement of the CCPA. (Edelman)

2.2.5. Lebanese Laws:

2.2.5.1. The Electronic Transactions and Personal data Law:

The E-Transactions Law was first introduced in 2004 but was passed 14 years later, making it outdated before being put into enforcement.

The E-Transactions law of September 2018 aims at regulating electronic commerce, giving it all the needed support, but disregarding data protection upon online commercial activity.

Personal data is defined as “any information that helps to directly or indirectly identify a natural person, by comparing the data or overlapping data collected from multiple sources”, but consent is not defined in this law.

In an article published by Smex organization in October 2018, it states that at the time of introducing this law, only 9% of the Lebanese population was using the Internet, compared to 76.1% in 2018 (Smex.org) . This is in addition to the fact that social media platforms did not exist at that time, which decreased the risk on users’ privacy and protection.

Article 92 of the law gives every natural person the right to objection upon collection and processing of their personal data, through commercial promotion, for legitimate reasons without identifying those reasons. Yet, the same Article prohibits the exercise of this right if the operation is under a legal obligation, or if it has been agreed upon.

The law gives a single executive authority, often the Ministry of Economy and Trade, the power to decide on data processing requests that are related to the collection, storage, or disclosure the data.

Article 95 giving the same authority such power, disregards the necessity of the involvement of the judicial authority or a specialized Data Protection authority.

Article 98 on the other hand, gives the same Ministry the right to decide on the requirements for authorization to make the data public or transferred.

Empowering a single executive authority, which would also be represented by the person of its Minister, leaves no doubt that the granted powers will be subject to abuse. Political, sectarian, and even personal interests or interferences will result in arbitrary determinations.

Articles 97 and 103 also give both Ministries of Interior and of defense the right to license processing personal data for "external and internal security of the state" (Smex.org) without informing the data subject concerned if that would endanger the objectives of the processing. Nevertheless what is considered "external or internal use" or what would "endanger the objectives of the processing" is not defined.

These provisions certainly pose a serious risk on the personal data collected and stored by companies, because, for example, public figures might be on good terms with and have mutual interests, or they might even be partners of. This will provide companies with the means to process personal data, identify and analyze users' interests, increase their customers, and achieve higher revenues. As a result, the success of those companies would empower the public figures involved with the businesses to take advantage of their positions or sensitive information related to people, and eventually have firm control over the society.

Another risk is privacy invasion for political purposes, which would mainly focus on preventing opposing points of views from rising against governmental practices.

Article 87 states that (Smex.org): "Personal data shall be collected faithfully and for legitimate, specific and explicit purposes.

The data shall be appropriate, not go beyond the stated objectives, be correct and complete, and remain on a daily basis as relevant as possible.

At a later stage, the said data may not be processed for purposes that are not in line with the objectives specified, unless this is related to processing data for statistical or historical purposes or for scientific research."

This article requires that data collection be for specific legitimate purposes explicitly according to stated objectives. However, it does not clarify what objectives are meant, neither what is considered legitimate, specific, or explicit.

On the other hand, article 94 provides for cases through which no permission for processing personal data is required, including educational purposes, non-profit organizational work, public records, and law enforcement. Paragraphs 5 and 6 of the same article do not require permission if the data subject was member or employed in a commercial company, or if the data subject was a client of similar companies.

In addition, it allows processing without permission if the council of Ministers issued a decree based on the proposal of the Minister of Economy and Trade deeming that processing personal data without the permission of the data subject shall have no risk to the private life or personal freedoms of the individuals.

This is considered a restriction to the users' right to object to processing their information, and allows processing institutions to refrain from informing users of their activity or taking their consent. Instead, it should be up to the data subject to decide whether to accept the collection and usage of their personal information.

The E-transactions law also does not give data subjects the right to withdraw their consent (Ducato) if previously given. This is regarded as a major concern for data protection, because it allows companies to take advantage of users' unawareness and limited knowledge to take control over their personal information.

Unlike the GDPR, this law does not establish clear provisions regarding the appointment of the data processing officer.

This law presents poor and undefined terminology, thus creating ambiguity upon deciding on the adopted standards, principles, limitations, and scope of application. The E-transactions law does not emphasize on the priority of protecting data in comparison with the previously discussed laws, rather it opens the door for companies and governmental authorities to decide on user data and control it.

There are many reasons that might have been the cause of this law, like its enactment fourteen years after introducing it, failing to appoint a specialized committee that has both technical and legal expertise to prepare a well-developed draft, or political pressure and personal interests. However, this does not exclude the opportunity to work on a new or updated law that is properly structured and developed to keep up with current regulations, in addition to establishing the infrastructure for its enforcement.

2.2.5.2. Consumer Protection Law of 2014:

The general objective of this law is to safeguard consumers' interests upon the sales of goods and services in Lebanon.

Article 12 of it requires the advertiser to prove the validity of the information available in the advertisement, and to provide the Consumer Protection Authority or the competent court looking into the case with the requested documentation.

In case of false or deceptive advertisements, the Ministry of Economy and Trade shall request correction, or the court dealing with the case may order to stop the broadcasting of the advertisement.

Article 26 of the law sets the cases that are considered arbitrary clauses, mainly giving the professional more power over the consumer, and creating an unbalanced relationship.

Articles 51 and 52 tackles the activities of the professional from a distance, including the Internet. However, it does not talk about the collected consumer personal data through trade, which could be used for advertising or third party operation purposes. The law focuses on the contractual information regarding the product or service traded. Article 58 of this law could be viewed as the closest to protection, as it provides that the contracting professional shall safeguard the collected information unless the consumer explicitly agrees otherwise. It also requires the professional to take all the measurements to ensure the confidentiality of the collected information. However, it is not clear whether those obligations are limited to the information obtained upon agreement, if they start from the negotiation period, or if the advertisement period is included as well. The article also addresses "the professional" without identifying if one of the parties only is the professional or both, leaving it subject to wider interpretation. Although Article 118 is titled "Consumer's Information", it establishes the punishment in case of refusal to supply consumers with the necessary information regarding the goods and services rather than consumers' personal data.

Chapter Three

Data Transfer through Commercial Activity

3.1. Case Study: Amazon

3.1.1. Its Establishment:

Amazon is one of the world's biggest companies. It was founded in 1995 by CEO Jeff Bezos as an online bookstore, for its annual revenue to reach $610 million in 1998 (Hall). As the company grew bigger, its activity expanded and it later launched its web services in 2002.

Today, Amazon has branched out to additional activities including software services, books, home appliances, automotive services, food, smart services, and it even offers live broadcasting.

3.1.2. Revenues and Profit:

Last year, the company's revenue reached $280.5 billion, with $11.5 billion net profit, making Jeff Bezos the World's richest man of real time net worth equal to $166.3 billion as of 7/1/2020 (forbes.com). Amazon has invested heavily in technologies, making the company an intersection of e-commerce and advertising (PATHAK).

Data Processing has allowed the company to expand its advertising activities that vary between its search engine, banner advertising, videos, and streaming services. In 2019, the company's ad revenues reached up to $4.8 billion for the quarter, making its annual ad revenue $14.1 billion, which summed up to 39% from the $10.1 billion in 2018

(Marvin). A report published on MarketingDive blog expects Amazon's ad revenues to increase by 470% until 2023 (Barry Levine on June 25). The company's successful rise has helped it gain loyal customers and encouraged other companies to spend their ad budgets on it (Masters).

On the other hand, Amazon's booming and expansion raises questions and concerns regarding user data.

3.1.3. Risks:

Upon going through the Website's Privacy Notice, it provided that the collection of customer personal information could be either given by the user, collected automatically, or collected from other services.

The list of sources and means of collecting user information reach up to 35 different ways, including interaction with Alexa services, contact upload, payment information, IP address, personal description and photographs. However, the notice does not clearly list all the information it collects and the sources it uses, instead it states "certain types of information" and gives "examples" of them. The use of indefinite terms is interpreted as a limitation to liability of the company.

Amazon uses its users' personal information for different purposes including personalization of services and products, and advertising. Although the company says it does not use information that directly identifies customers, it works with third parties to provide interest-based ads, and collect information at the same time using cookies and similar technologies. It also gives users the right to choose not receiving interest-based ads (Amazon.com).

However, the privacy notice clearly states that in case of refraining from providing "certain information, the customer might not be able to take advantage of many of the Amazon Services and it recommends keeping cookies and identifiers on"[Privacy notice/ What choices do I have?]. Furthermore, the company preserves a copy of the customer's previous records even after the latter updates his/her information.

User data is shared with third parties, third-party service providers, business transfers, and for protection or law compliance purposes.

In 2019 alone, it has been revealed that Amazon permitted employees to access video feeds from Ring cameras even when not necessary (Rens). As previously mentioned, third parties could be police departments or governmental agencies. Amazon has signed contracts with Oregon sheriff department to supply it with facial-recognition services, and has won a bid worth $600 million with the CIA. Those are two examples of many contracts that the company enters with various parties.

Although it might be putting all its efforts to comply with regulations like the GDPR and the CCPA, it remains subject to risk of cyber-attacks. Such threats constitute data subjects' main concerns as to who their information might end up with and in what ways they could be harmed.

3.1.4. Suggestions:

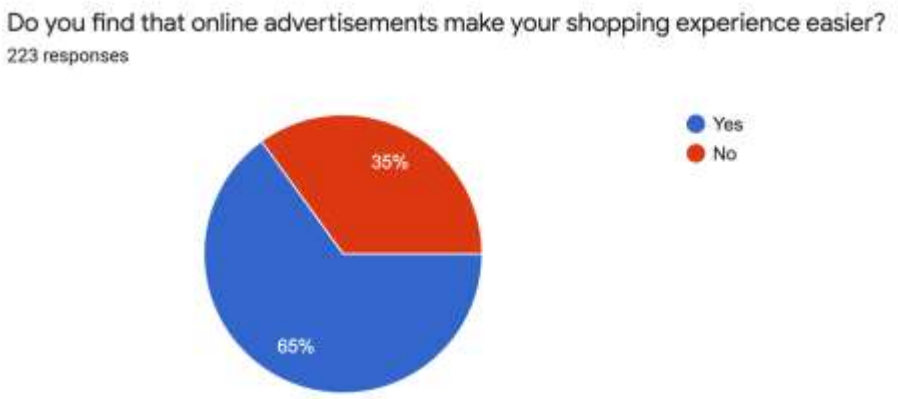
The proper implementation of the existing laws is vital for Amazon and similar corporations. We cannot deny the fact that they have substantially contributed to the development of the World economy, particularly the digital economy. They have facilitated shopping experiences, created millions of job opportunities, supported

globalization, and removed borders between countries. Nevertheless, without putting people's privacy at risk this might not have been possible. Therefore, regulations that protect people's rights and interests and ensure their safety shall be appropriately enforced.

The proper enforcement of law also ensures those companies' continuation and encourages innovation. It protects them from cyber-attacks putting them under major loss, and at the same time builds a relationship based on trust with users.

3.2. The Risks Involved:

The ongoing development of new technologies throughout the past decade has emphasized the essential role the Internet is playing. People all over the world are becoming more reliant on services provided through the Internet. New technologies have positively impacted information flow, online trade, job opportunities, and international communication. In the graph below, 65% from a total of 223 responses found that online advertisements make their shopping experience easier (Graph 1).



Graph 1: The Effect of Online Advertisement on the Shopping Experience

With globalization of production, the flow of data and information across borders has become vital for all economic sectors (I. Commission). In addition, the Internet has opened the door for small to medium sized (SMEs) enterprises to build their businesses and compete with larger companies (Chi).

The telecommunications company Verizon purchased AOL for $4.4 billion because of the company's CEO that was previously the first head of advertising sales at Google. (S. Zuboff). This establishes that companies consider online advertising a key player in their activity, where data flow and processing is a main part of its success, but at the same time raises awareness to the risks of companies' activities in online marketing.

These risks could be: - Privacy invasion

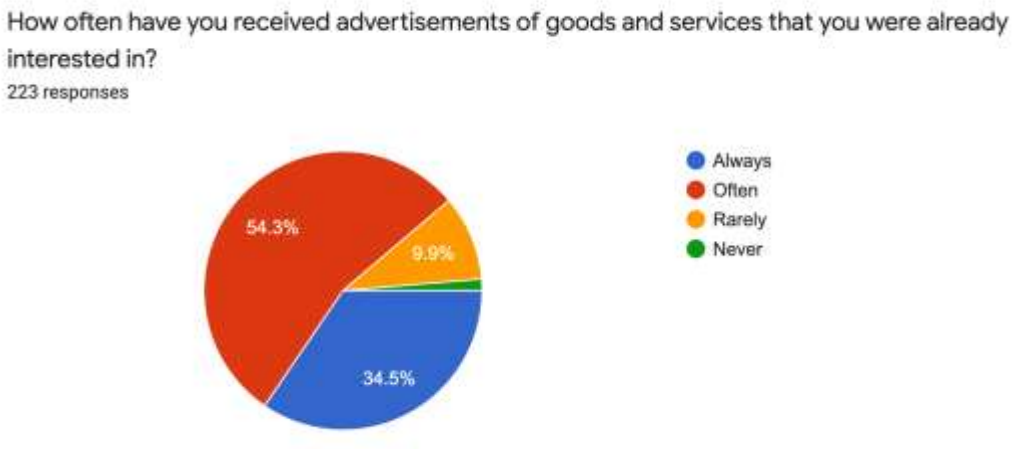
- Cyber-Crimes
- Political Influence
- Governmental Control
- Competition

3.2.1. Privacy Invasion:

Last week, while searching for planning agencies, my Instagram feed was full of sponsored ads of venues, photographers, catering services, and so on. This often happens nowadays, whether it is on Instagram, Google, Facebook, and even if the search was not initiated on the same website or application.

In a survey completed by 223 people, one the questions was "How often have you received advertisements of goods and services that you were already interested in?"

88% of the responses ranged between always and often receiving such advertisements (Graph 2).



Graph 2: The percentages of receiving targeted advertisements

Online users have become familiar with being tracked once they click on their screen, but people might not be aware that software companies track users' movement of the mouse. It helps them analyze the user's health state to the extent of identifying if he/she is an alcoholic or not (Tiku). Reaching sensitive information, alongside with the previously piled data from other sources, companies build user profiles allowing them to sell the gathered information to both alcohol and pharmaceutical companies in the geographic area of the user.

Similar repetitive scenarios have caused fear within users and raised multiple questions. Online users are worried about how their personal data is being used, why it is being collected, who is receiving it, and for how long would it last with companies.

While some people might be okay with their data being stored and used because they believe there is nothing to do about it, or they accept such operations as long as they are

not being directly harmed, it still constitutes an invasion of privacy. Users' very personal information could be identified by companies, thus exposing their vulnerabilities to parties they might not even know they exist.

Amazon, for example, knew that a customer was pregnant before she knew herself. They reached the conclusion when the customer's behavior changed, because pregnant women usually reject certain products, so they began sending her personalized advertisements for newly born products (DW Documentary). Google also sold thermostats that secretly included microphones for years (Rens).

To honor privacy, even if there is no direct danger, is a fundamental principle both ethically and legally. The concerned individual shall decide what to do and who to give access to his/her personal information after being fully aware and informed of the implications of their decision. However, as mentioned above, companies might not respect their obligations, which leaves it to the supervisory authorities to always take all the necessary measurements for safeguarding citizens and their basic civil rights.

3.2.2. Cyber-Crimes:

Although companies processing data for advertising purposes are professionals, and are thus legally required to take all the necessary precautions to protect personal data and ensure its safety, the digital world remains uncertain and subject to cyber-attacks.

The increasing activity online increases the risk of content piracy. The FBI reported that nine out of 10 US companies experienced computer security incidents in 2005, leading to $67.5 billion in loss (Kshetri), and leaving US businesses in fear of cybercrimes more than traditional crimes.

Cybercrimes are increasing continuously, and with the development of data processing, it imposes a greater threat on both consumers and companies. Processors and controllers will be questioned by users and even investors in case of cyber-attacks, which would affect their credibility. On the other hand, Users' personal data would be exposed, making them subject to fraud, identity theft, stalking, sexual harassment, and threats to reputation or physical violence. This is a serious matter that millions of people around the world are suffering from even though it is still not very common publicly talk about.

It is not necessary for companies to be intentionally involved in similar crimes, but the company's negligence or mismanagement could sometimes result in the leak of information it stores or uses for advertising purposes to criminal organizations or to the public directly.

Exposing users' secrets and fears, or threatening to do so might ultimately lead to the death of the victims, who often resort to suicide or could be killed by the criminals themselves. In some societies for example, exposing an individual's sexual orientation might put him/her in danger of being killed by their families or arrested by authorities. Losing one's life cannot be compensated, and here lies the vitality of securing users' data.

In 2019, data of 419 million facebook users were leaked including phone numbers, user names, gender, and location by country. This happened even after facebook announced that it was making changes to better protect people's information (Davey Winder).

Such alarming incidents stress on the importance of maximizing efforts to protect user data, because if the world's strongest companies like facebook are facing massive

violations, whether intentionally or unintentionally, the concern about people's safety increases.

3.2.3. Political Influence:

Amul Kalia, an analyst and intake coordinator at the Electronic Frontier Foundation (Grauer), pointed out that election campaigns in the US use information from data broker companies to determine who to target in ads (Grauer). Just as companies have great impact and control over the regulatory activity, politicians, particularly election candidates, are customers of data processors and data brokers. They benefit from piling their country's user data in order to tailor electoral campaigns that talk to people's interests, needs, fears, and aspirations. This is the same as the activity of commercial companies that use data subjects' information for targeted advertisements of goods and services. Data Brokers are companies that collect user data from multiple sources including websites, applications, and public records. After that, they add those records and sell them to third parties which could be retail companies, governments, or politicians.

The Cambridge Analytica scandal is one of the most popular cases through which users' personal data were used for election campaigns. The company, Cambridge Analytica, collected the users' personal data from their facebook accounts and used it to target individuals for the Trump 2016 Presidential Campaign. The use of targeted ads helped them influence people to vote for Trump and eventually win the elections (Rehman).

The risk of political influence upon collecting personal data and personalizing campaigns according to people's individual fears could raise questions of whether the

politician is building his/her success on strengthening voters' vulnerabilities rather than introducing real development plans serving the wellbeing of the society.

Therefore, it is essential that people's information be protected. This does not mean that political parties cannot learn about their audience's fears and needs, but this knowledge shall be gathered through information already made available to the public, not the personal data of every individual.

3.2.4. Governmental Control:

Governments nowadays use public interest as a reason to collect the personal data of their residents from processing companies. Although maintaining national security and preventing crimes are fundamental principles, governments often tend to abuse their power, jeopardizing civil liberty. Article 19 of the International Covenant on Civil and Political Rights, Article 10 of the EU Convention on Human Rights, and Article 13 of the American Convention of Human Rights all emphasize on the right to freedom of expression. However, law enforcement often varies by country or region, and although the majority of countries acknowledge freedom of speech, governments do use users' data, whether they do it publicly or secretly.

The Chinese government has a history of arresting protestors through tracking them from their IP addresses and facial recognition softwares. As a result, protesters resort to covering their faces and trying to avoid using technologies that might help identify them. On the other hand, while the United States of America is one the world's top freedom of expression advocates, its authorities rely on online data processing to reach its residents' personal information.

Other than law enforcement orders, governments sign contracts with processing companies to have access to their data basis. In 2013, Amazon won a $600 million worth bid for a 10-year contract with the CIA (Charles Babcock). Furthermore, Oregon's sheriff department was the first law enforcement agency in the US to use Amazon's facial-recognition software to help solve crime (Fowler).

The concern in those cases is that contracting authorities might tend to take arbitrary action of illegitimate basis, using the collected data. Such orders or actions that could lead to the loss of lives or oppression, might be driven by personal incentives of employees in the authority or by political parties supporting the government to put an end to opposing points of view. The data could also be used by third parties like spying agencies or enemy countries to cause threats to national security.

Building solid relationships between companies and governments, both being in strong positions, leaves users at a weaker position and incapable of restoring their rights. This is considered a matter of democracy and basic civil rights that calls for rightful enforcement of privacy and data protection laws.

3.2.5. Competition:

A report published in 2019 by the Economic Times states the following: "The 'Seven Super' companies – Microsoft, Apple, Amazon, Google, Facebook (all US based) and China's Tencent and Alibaba – account for two-thirds of the total data market by value, according to a recent report by UNCTAD on the digital economy.

Google has some 90% of the market for internet searches, Facebook accounts for two-thirds of the global social media market and is the top social media platform in more

than 90% of the world's economies. Amazon boasts an almost 40% share of the world's online retail activity and its Amazon Web Services accounts for a similar share in cloud services, the report said." (Mankotia)

The numbers provided in the above paragraph are sufficient to prove the dominance of those giant companies on the World's digital economy. The shift from traditional contextual marketing towards behavioral marketing has opened the door for those companies to grow into becoming the World's wealthiest.

Although digitalization has given small to medium sized enterprises opportunities to establish successful businesses, big multinational corporations are still in control of the economy. Amazon, for example, which started as a retail company, has now branched out to provide smart services, books, pet care, home appliances, automotive services, live broadcasting, foods, and software services. The website has become so abundant in its services, it is almost a world in itself. One example of the company's dominance is its intense advertisement of Kindle e-books, which noticeably increased its publishing activity, but in return disrupted the book-publishing market (Hall).

With this expansion, and using targeted personalized advertising, the company can know everything about the users' needs and interests, knowing that this could be achieved from its own branches alone without the third parties that it might be collaborating with. The company's wide activity allows it to supply users with all their goods and services, especially if they get used to dealing with the same company and finding their needs on its website.

This will eventually encourage consumers to let go of small and medium sized businesses, retail or local, because they actually find it easier to get all what they need through Amazon or Alibaba for example, where the probability of receiving discounts and offers is also higher.

While we might believe we are only consumers and customers of those companies, we are actually raw material suppliers. Without our data and the targeted behavioral advertisements based on it, companies would have to put in all their efforts to compete with each other fairly. SMEs will be able to take their chances in the market and strive to achieve their best without being under the control of giant corporations. Therefore, implementing the right regulations to ensure a fair competition and to limit any monopoly or duopoly is a must. Protecting and supporting SMEs shall be pointed out to encourage innovation within societies.

3.3. Recommendations and Suggestions

There are different ways through which governments and companies can follow to protect privacy of users, and ensure the continuity of business.

This could be established through: -Building Trust

-Raising Awareness

- Establishment of the Competent Supervisory and Enforcement Authorities

-Balancing between Privacy and Digital Economy

-Opting for Non-Tracking Services

3.3.1. Building Trust:

Building trust between both users and companies from one side, and users and governments from the other side are very important for businesses to succeed, users to feel safe, and governments to reserve their people's respect.

Trust and good reputation are main factors that contribute to the success of businesses and commercial activities, paving the way to gain loyal consumers and build good relationships.

Brand Imaging is one of the ways that positively affect perceived effectiveness of business privacy policies and perceived benefits of information disclosure [n.Journal of theoretical]. A favorable brand image within consumers encourages them to believe that the particular brand they are dealing with would not use their personal information for purposes other than those declared by the company, or in ways that might endanger individuals. This constitutes part of the trust relationship between a business and its consumers or perspective customers, alongside with the business' operation in good faith to ensure its consumers' best service. Therefore, the favorable practice and good reputation of a company will support its activity, and decrease the concerns or risks it faces.

Trust is not only essential between a business and its consumers, but the government also plays a positive role in establishing trust. When companies trust that the government is fair and would implement the laws properly, they will be willing to cooperate with it for a better enforcement that does not harm their business activity. Furthermore, when the government fulfills its obligations towards its people properly,

people will have to worry less about what to do to protect their information from abuse and will trust the authorities in their safeguarding.

Similarly, when governments and consumers trust companies to implement the law properly and perform their practices respectfully, the concern about data protection and privacy risk will decrease.

Each of the government, companies, and consumers are key players in building a healthy relationship based on trust that ensures continuity, innovation, and providing the mutual interests of all the concerned parties.

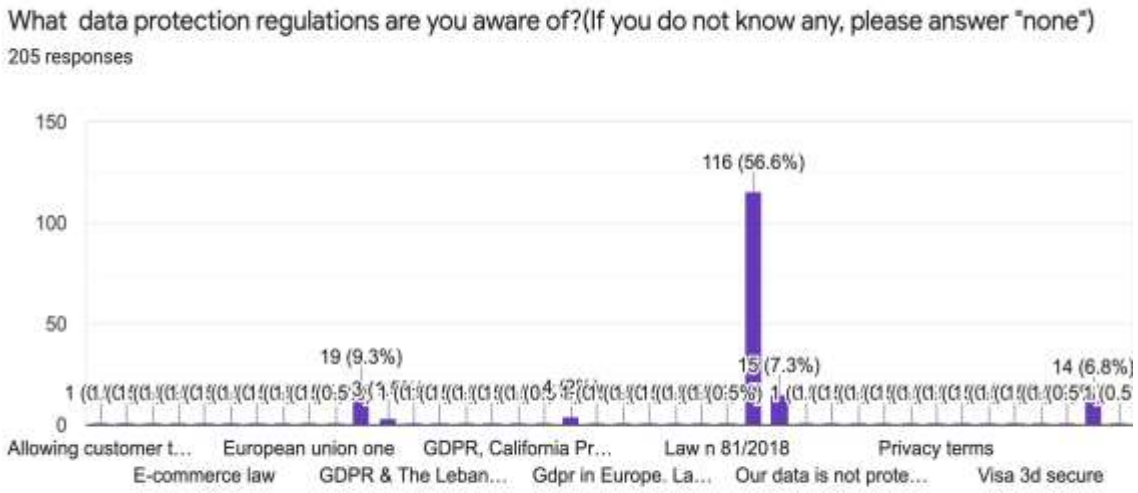
3.3.2. Raising Awareness:

While the role of the Internet is constantly rising in our daily operations, concerns about privacy and data protection rise in parallel. However, not all users have sufficient knowledge about the occurring processes often dealing with their personal data.

Online users, companies, and governments all have duties that complete each other. Users on one hand shall ask about online operations to be able to understand the process, its implications, and how it affects their personal data. However, governments and companies have higher obligations to inform users and consumers of the different aspects of online activity because they are considered professionals. Therefore, it is their responsibility to explain to data subjects how they collect their data, the purposes of collection, and to clarify the users' rights and obligations in a clear and unambiguous manner that is easy to understand by the public.

The below graph reveals the critical need for raising awareness in Lebanon. As the majority of the respondents do not know any data protection regulations, the GDPR

comes in second place at the time when the survey was directed to Lebanese citizens and residents, whereas very few are aware of the Lebanese E-Transactions Law of 2018. A considerable percentage of the responses provided general terms such as privacy, data protection, or e-commerce, but did not identify any particular law. The alarming results call for immediate action towards raising awareness about data privacy laws related to the commercial activity, which allows users to learn about their rights and stress on companies performing their obligations (Graph 3).



Graph 3: The knowledge of data protection regulations

3.3.3. Establishment of the Competent Supervisory and Enforcement Authorities:

In Europe, the GDPR provides for the establishment of a competent supervisory authority in each Member State, in addition to the establishment of the European Data Protection Board", responsible for coordination between all supervisory authorities across the Union.

In UK, the ICO is the body in charge of data protection and privacy regulation, and the FTC is the framework set to help businesses comply with the current laws.The laws protecting data in the region are well-developed and deal with the matter in detail, from its different aspects.

However, in Lebanon this is not the case. The E-Transactions Law of 2018 does not clearly set the rules for appointing the data processing officer from one side, and give excessive power to the executive authority, often the Ministry of Trade and Economy from the other side. Other than the fact that such weak distribution of power increases the concern of arbitrary decisions, the appointed authorities for decision making might lack the competence and expertise to take the right decisions.

Thus, because a strong and healthy supervisory body is the foundation of a well-applied laws, it is necessary to follow objective criteria for the appointment of individuals in decision making positions. Companies shall also appoint data governing bodies with law compliance officers that audit and report the company's activity periodically.

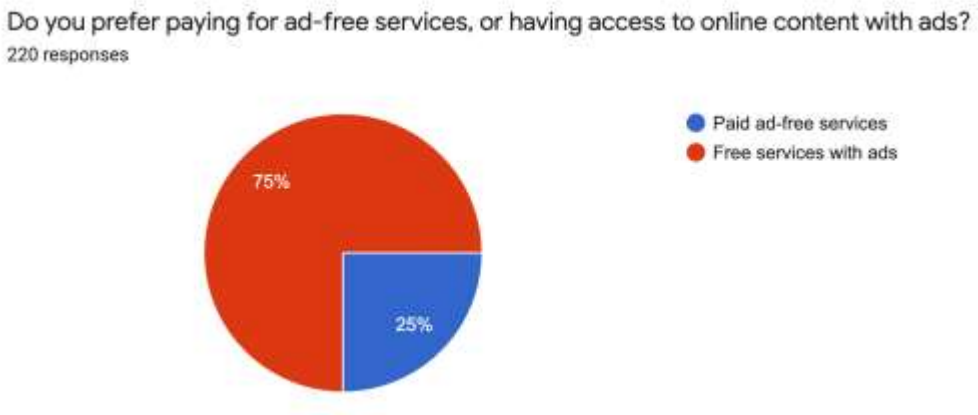
3.3.4. Balancing between Privacy and Digital Economy:

Without a healthy economy and civil rights, societies are at high risk of falling apart. Privacy of personal information is a basic civil right that the individuals shall be able to decide whether to give up or would rather preserve it. It is the businesses' obligation to give users all the information needed to take an informed decision, and if it is not possible for them to perform their activities without obtaining personal data then businesses shall make it clear to the users. Then, it would be for the data subject to decide upon his/her priorities.

Strict and disruptive regulations could negatively affect those companies while they are directly contributing to the turnover of the economic cycle. In this regard, the ICC recommends that governments strive to achieve balance between individuals and businesses by building trust between both sides, encouraging the adoption of favorable conditions of the digital economy and data-driven innovations, and taking into account the interests of the individuals (I. Commission).

3.3.5. Opting for Non-Tracking Services:

Opting for Non-Tracking services could be considered for a lot of people as the last choice. Many might find it difficult to shift from using a server to another after having their information already uploaded to one, or after being used to working from the initial one. Others are okay with having ads follow them around as long as they receive free online content, which is the case in the graph below:



Graph 4: The preference of paid ad-free services vs. access to free online content with ads.

However, if the risk of privacy invasion or disclosure of personal information to third parties is a main concern for users, they still have other options to use. DuckDuckGo is

a search engine, similar to Google, but instead of using behavioral advertising the company opts for contextual advertising. The company still makes its money from advertising, but when the user searches for a product, for example, ads appear on the screen of the same page without following him/her from one place to another (Burgess). DuckDuckGo might not be achieving the revenues Google is achieving from targeted advertisements, but it still is a successful business for performing its purpose without storing personal data and by blocking the invisible trackers hidden on web pages.

Chapter Four

Conclusion

With globalization and digitalization, cross-border data flow has become a main part of companies' operation. As shown in this research, companies rely heavily on processing data subjects' personal information to achieve unprecedented revenues, but this has also increased the concerns of individuals about their personal data.

We cannot deny the importance of both businesses and privacy, which calls for the proper implementation of laws like GDPR and similar regulations. In Lebanon however, there is a need for updating the current regulations to keep up with international standards and practices, and most importantly those laws shall be enforced appropriately under supervision.

The ultimate solution might be achieving harmonization in regulation across all countries, without differentiating between societies according to race or region, because data flow is not limited to one country or region. This could be established when governments cooperate to enter a unilateral convention that best serves all interests.

Yet, the question remains if this is possible anytime soon with the continuous growth of tech companies and their power to influence and shape societies?

References

Amazon.com. https://www.amazon.com/gp/help/customer/display.html?nodeId=202075050.

Barry Levine on June 25, 2019. *marketingdive.com/ Amazon's ad revenues to grow 470% by 2023*. 25 June 2019. https://www.marketingdive.com/news/amazons-ad-revenues-to-grow-470-by-2023-study-finds/557531/

BARRY, ELIZABETH POLLMAN and JORDAN M. "Regulatory Entrepreneurship." *Southern California Law Review, Vol. 90* (n.d.): 383.

BURGESS, MATT. "What is GDPR? The summary guide to GDPR compliance in the UK." 24 March 2020. *wired.co.uk.* https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Burgess, Matt. *wired.co.uk; Google got rich from your data. DuckDuckGo is fighting back*. 8 June 2020. https://www.wired.co.uk/article/duckduckgo-android-choice-screen-search

Charles Babcock, on 11/08/2013. *informationweek.com, Amazon Again Beats IBM For CIA Cloud Contract;* . 11 August 2013. https://www.informationweek.com/cloud/infrastructure-as-a-service/amazon-again-beats-ibm-for-cia-cloud-contract/d/d-id/1112211

Chi, by Melody Y. Kiang and Robert T. "A FRAMEWORK FOR ANALYZING THE POTENTIAL BENEFITS OF INTERNET MARKETING,." *Journal of Electronic Commerce Research, VOL. 2, NO. 4* (2001): 157.

Commission, Federal Election. "REPORT OF COMMUNICATION COSTS." 2001. *fec.gov.* https://www.fec.gov/resources/cms-content/documents/fecform7.pdf

Commission, ICC. "Trade in the Digital Economy, A Primer on Global Data Flows." Primer. n.d. Document.

Commission, The Federal Election. "Presidential spending limits for 2016." official website. 2016. **https://www.fec.gov/help-candidates-and-committees/understanding-public-funding-presidential-elections/presidential-spending-limits-2016/**

Davey Winder, September 5,2019. *Forbes.com, Unsecured Facebook Databases Leak Data Of 419 Million Users*. 5 September 2019. https://www.forbes.com/sites/daveywinder/2019/09/05/facebook-security-snafu-exposes-419-million-user-phone-numbers/#2bb098461ab7

DW Documentary. "Amazon, Jeff Bezos and Collecting Data." Documentary. 2019. Youtube Documentary. https://www.youtube.com/watch?v=O90PShJVu58&t=1s

Edelman, Gilad. *wired.com; California's Privacy Law Goes Into Effect Today. Now What?* 1 January 2020. https://www.wired.com/story/ccpa-guide-california-privacy-law-takes-effect/

fec.gov. *Public funding of presidential elections*. n.d. https://www.fec.gov/introduction-campaign-finance/understanding-ways-support-federal-candidates/presidential-elections/public-funding-presidential-elections/#:~:text=Although%20an%20individual%20may%20contribute,%245%2C000%20threshold%20in%20each%20state.

forbes.com. *forbes.com/profile/jeff-bezos/*. 7 January 2020. https://www.forbes.com/profile/jeff-bezos/#7daefd261b23

Fowler, Geoffrey. *washingtonpost.com, The Washington Post: Goodbye, Chrome: Google's Web browser has become spy software*. 21 June 2019. https://www.washingtonpost.com/technology/2019/06/21/google-chrome-has-become-surveillance-software-its-time-switch/

Grauer, Yael. *vice.com-What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?* 27 March 2018. https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection

Hall, Mark. *britannica.com/Amazon.com American company*. 9 April 2020. https://www.britannica.com/topic/Amazoncom

i-scoop.eu. *Personal data protection: data subject, personal data and identifiers explained*. n.d. https://www.i-scoop.eu/gdpr/gdpr-personal-data-identifiers-pseudonymous-information/.%20n.d

Jen Pollakusky, Michael Hornsby. "Ineffective Election Monitoring in Lebanon Highlights Urgent Need for Independent Body." press. 2018. **https://www.transparency.org/en/press/ineffective-election-monitoring-in-lebanon#**

Kshetri, Nir. "Positive externality, increasing returns, and the rise in cybercrimes." *Communications of ACM, vol.52, no.12* (2009).

Lesley Sutton, Nikhil Shah and James Lamberton. *ePrivacy Regulation – what next?* 7 January 2020. **https://www.gtlaw.com.au/insights/eprivacy-regulation-what-next**

macrotrends. "Amazon: Number of Employees 2006-2020 | AMZN." Study charts. n.d. https://www.macrotrends.net/stocks/charts/AMZN/amazon/number-of-employees

Mankotia, Anandita Singh. *economictimes.indiatimes.com/ Govt may soon make it mandatory for Google, Facebook to sell users' public data*. 9 September 2019. https://economictimes.indiatimes.com/tech/ites/tech-companies-may-have-to-provide-access-to-non-personal-data/articleshow/71041298.cms

Marvin, Ginny. *marketingland.com/Amazon's booming ad business grew by 40% in 2019;* . 3 February 2020. https://marketingland.com/amazons-booming-ad-business-grew-by-40-in-2019-275312

Masters, Kiri. *Forbes.com; Why Brands are Flocking to Amazon Advertising*. 20 Februrary 2019. **https://www.forbes.com/sites/kirimasters/2019/02/20/why-brands-are-flocking-to-amazon-advertising/#3a2be19260db**

PATHAK, SHAREEN. *DIGIDAY.com/ THE AMAZON EFFECT; How Amazon is readying its blitz on the ad industry*. 5 October 2017. https://digiday.com/marketing/amazon-will-soon-2000-people-advertising-new-york-city/

Rehman, Ikhlaq ur. "Facebook-Cambridge Analytica data harvesting:." *University of Nebraska- Lincoln* (2019): 1-11.

Rens, Andrew. " WHO IS IN CHARGE HERE? THE INTERNET OF THINGS, GOVERNANCE AND THE GLOBAL INTELLECTUAL PROPERTY REGIME." *UCLA Journal of Law & Technology:* (2019).

Richter, Brian K. "Case Study: Do Business and Politics Mix?" *Harvard Business Review* (2014). https://hbr.org/2014/11/do-business-and-politics-mix

Smex. *An "Ugly" New Data Protection Law in Lebanon*. News. Beirut: Smex, 2018. **https://smex.org/an-ugly-new-data-protection-law-in-lebanon/**

Tiku, Nitasha. *wired.com, The Dark Side of 'Replay Sessions' that Record Your Move Online*. 11 June 2017. **https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/**

UK, IAB. "Digital advertising guidance: cookies, consent & the GDPR." 4 March 2020. *iab UK.*

Zuboff, Professor Shushana. *Shoshana Zuboff on 'surveillance capitalism' and how tech companies are always watching us* 4 News Channel. 23 September 2019. https://www.youtube.com/watch?v=QL4bz3QXWEo

Zuboff, Shoshana. "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power." Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. 2019.

Legal Sources:

The GDPR;

The New ePrivacy Regulation proposal;

The PECR;

The CCPA;

The Lebanese E-Transactions Law of 2018; and

The Lebanese Consumer Protection Law of 2014