

LEBANESE AMERICAN UNIVERSITY

Legal Frameworks Governing Social Data Analytics and Privacy Concerns
among Social Media Users

By

Youssef Ramzi Mansour

A thesis

Submitted in partial fulfillment of the requirements

For the degree of Master of Business in Law

Adnan Kassar School of Business

April 2019

© 2019
Youssef Ramzi Mansour
All Rights Reserved

THESIS APPROVAL FORM

Student Name: Youssef Ramzi Mansour I.D. #: 201706482

Thesis Title: Legal frameworks governing social data analytics and privacy incident among social media users

Program: Business Law

Department: Information Technology and Operations Management

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:

Masters in the major of Business Law

Thesis Advisor's Name: [Redacted]

Signature: [Redacted] Date: 16 / 04 / 2019

Committee Member's Name: Abbas Tarhini

Signature: [Redacted] Date: 16 / 4 / 2019

Committee Member's Name: Khaled Fakih

Signature: [Redacted] Date: 16 / 4 / 2019

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: Youssef Ramzi Mansour

Signature: 

Date: 10 / 04 / 2019
Day Month Year

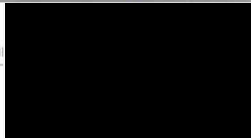
PLAGIARISM POLICY COMPLIANCE STATEMENT

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: Youssef Ramzi Mansour.

Signature



Date: 10 / 04 / 2019
Day Month Year

ACKNOWLEDGEMENT

This thesis was achieved by the guidance and support of many people.

Many thanks are due to my advisor Attorney William Melki, who guided me throughout the process, always taking into consideration my best interest. I thank him with all my heart.

I would like to thank my committee members Dr. Khodr Fakih and Dr. Abbas Tarhini for their care, effort and time.

I deeply thank members of my family, especially my parents Ramzi and Daed, my sister Rim, my brother Rayan, my uncle Jamal Mansour and his wife Fadoie Mardam-Bey for their constant support.

Finally, I want to thank my friends Sary Rizk, Dr, Tarek Kazoun, and Ali Dakroub for being there for me in times of need.

Legal Frameworks Governing Social Data Analytics and Privacy Concerns among Social Media Users

Youssef Ramzi Mansour

ABSTRACT

Big data is a relatively new concept that refers to the enormous amount of data generated in a new era where people are selling, buying, paying dues, managing their health and communicating over the internet. It becomes natural that generated data will be analyzed for the purposes of smart advertising and social statistical studies. Social data analytics is the concept of micro-studying users interactions through data obtained often from social networking services, the concept also known as “social mining” offers tremendous opportunities to support decision making through recommendation systems widely used by e-commerce mainly. With these new opportunities comes the problematic of social media users privacy concerns as protecting personal information over the internet has become a controversial issue among social network providers and users. In this study we identify and describe various privacy concerns and related platforms as well as the legal frameworks governing the protection of personal information in different jurisdictions. Furthermore we discuss the Facebook and Cambridge Analytica Ltd incident as an example.

Key words: Big data, Social data, Social data analytics, Privacy concerns, Laws and regulations, Social networking services.

TABLE OF CONTENTS

Chapter	Page
I. Introduction to Social Data Analytics.....	1
1.1. Big Data.....	1
1.1.1. Definition.....	1
1.1.2. Characteristics.....	1
1.1.3. Applications.....	2
1.1.4. Social Data Revolution.....	3
1.2. Types of data.....	4
1.3. Social data and the business sector.....	5
1.4. Computational social science.....	6
1.5. Social Data Analytics.....	6
1.6. Obtaining social data.....	7
II. Privacy concerns and related platforms.....	8
2.1. Introduction.....	8
2.2. Causes of online privacy concerns.....	9
2.2.1. Overlook.....	9

2.2.2. Offering multiple levels of privacy.....	10
2.2.3. Public behavior concern.....	10
2.2.4. User awareness in social networking services.....	11
2.3. Data access methods.....	11
2.3.1. Data sharing with third parties.....	11
2.3.2. Application programming interface.....	12
2.3.3. Search engines.....	13
2.3.4. Location data.....	13
2.4. Potential Dangers.....	13
2.4.1. Identity theft.....	13
2.4.2. Preteens and early teenagers.....	14
2.4.3. Sexual predators.....	15
2.4.4. Stalking.....	15
2.4.5. Unintentional fame.....	17
2.4.6. Job market and workplace discrimination.....	17
2.4.7. Online victimization.....	18
2.4.8. Commercial tracking.....	19
2.4.9. Surveillance.....	19
2.4.10. Invasive privacy agreements.....	20
2.5. Social networking platforms.....	21
2.5.1. Facebook.....	21
2.5.2. Instagram.....	22
2.5.3. Twitter.....	22

2.5.4. Snapchat.....	23
2.6. The Facebook and Cambridge Analytica case.....	24
2.6.1. Facts and process.....	24
2.6.2. Impacts and responses.....	25
2.6.2.1. Facebook.....	25
2.6.2.2. Cambridge Analytica.....	25
2.6.2.3. Governments.....	26
2.6.2.4. The public in general.....	26
2.7. Facebook testimony to US Congress.....	27
III. Social data privacy laws: a global comparative approach.....	29
3.1. The United States of America.....	29
3.1.1. Relevant legal frameworks today.....	29
3.1.1.1. The Privacy Act of 1974.....	29
3.1.1.1.1. Conditions of disclosure.....	30
3.1.1.1.2. Department of Justice.....	31
3.1.1.1.3. Computer Matching and Privacy Protection Act.....	31
3.1.1.1.4. Access to records.....	32
3.1.1.2. Several attempts of regulations.....	32
3.1.1.2.1. Child Online Protection Act (COPA).....	32
3.1.1.2.2. Social Networking Online Protection Act.....	33
3.1.1.2.3. Password protection Act of 2012.....	34
3.1.1.2.4. Social Media Privacy Protection and Consumer Right Act of 2019.....	35

3.1.1.2.5. Social Media Use in Clearance Investigations Act....	36
3.1.1.2.6. Data Privacy Act.....	36
3.1.1.2.7. Protecting Consumer Information Act of 2019.....	38
3.1.1.2.8. Commercial Facial Recognition Act of 2019.....	38
3.1.2. Regulation examples at the state level.....	38
3.2. The European Union: General Data Protection Regulation (GDPR).....	40
3.2.1. Introduction.....	40
3.2.2. Scope.....	42
3.2.3. Legal basis for “processing”	43
3.2.4. Accountability.....	44
3.2.5. Data Breaches.....	46
3.2.6. Penalties.....	46
3.2.7. Exemptions.....	47
3.2.8. Impacts of the GDPR.....	47
3.3. The United Arab Emirates.....	48
3.4. Lebanon.....	50
Conclusion.....	52
References.....	54-70

Chapter One

Introduction to social data analytics

1.1. Big data:

1.1.1. Definition:

The term “Big Data” was initially used in the 1990s and popularized by John Mashey, (Ph.D. in computer sciences). A large set of structured and unstructured data forms big data which makes it beyond the capabilities of traditional software to process it within a tolerable amount of time. The scale of the information contained in big data is exponentially increasing from a few exabytes in 2003 to several thousand of exabytes in 2019 which requires a unique technology to manage.

One definition concluded in 2016 that "Big data represents the information assets characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value." Another definition for big data provides that big data is "data sets characterized by huge amounts of frequently updated data in various formats, such as numeric, textual, or images/videos."

Another definition in 2018 concluded that "Big data is where parallel computing tools are needed to handle data. This represents a distinct and clearly defined change in the computer science used, via parallel programming theories, and losses of some of the guarantees and capabilities made by Codd's relational model."

1.1.2. Characteristics:

“Volume, Variety, Velocity and Veracity” (or the four Vs) are the basic characteristics of big data.

To be considered “big data”, the volume of data generation and storage should be in several exabytes. Furthermore, datasets containing text, images, audio, and video help analysts to effectively use resulting insights.

The frequency of data generation and the frequency of storing, processing and sharing the data are two components of “Velocity” characterizing big data, therefore obtaining data in real time is crucial for analysts to achieve effective data insights and conclusions.

Data veracity refers to its value and quality which can alter the accuracy of conclusions achieved by analysts from interpreting the data since it varies immensely.

1.1.3. Applications:

Data management specialists became a crucial need for software companies (Microsoft, Oracle Corporation, Dell...) which spent more than \$15 billion hiring corporations specifically to process and analyze online data to the extent that the data analysis industry reached \$100 billion in 2010 with yearly growth of 10%.

Estimates show that a third of the information being exchanged online is text or images which are the most useful types of data for analysts due to the ease of processing, but this only shows how promising unused audio and video data formats can be when bringing in special sets of algorithms in order to attain ease of access and processing.

Data traffic through telecommunication worldwide reached 281 petabytes in 1986, 471 petabytes in 1993, increasing to 2.2 exabytes due to the appearance of web 2.0 networking services in 2000, 65 exabytes in 2007, 1 million exabytes in 2014, 1.1. zetabytes in 2016, and the forecasted amount of data online in 2019 could reach up to 2 zetabytes.

The applications of big data cover governmental bodies, world development, productive industry, health, education, media, insurance, internet of things (IoT) and information technology (IT).

1.1.4. Social data revolution:

With time, more sophisticated social networking services appeared like twitter where sharing a tweet became equivalent to sending a text message and every tweet has the potential to be seen by the public allowing a user-world interaction, and Facebook where users are allowed to share their private information with friends allowing a user to user interaction as well as the option of a user-world interaction according to privacy settings provided by Facebook and approved by the user.

Craigslist and the wishlists of Amazon are the founders of online data sharing providing information and reviews submitted by users to anyone asking for it, even the job market is being shaped based on information users share online on social networking services.

The social data revolution triggered by social networking services appearing in the 2000s is the shift from direct personal human interaction into private online data sharing which resulted in a phenomenal amount of publically disclosed online data.

This form of communication was rendered unfeasible when it comes to overheads but with technological advances leading to the rise of social networking sites between the years 2004 and 2010, made a wider platform of data sharing possible.

This shift incorporated the appearance of social networking services made possible by the creation of web 2.0 considered as the “catalyzers” of online data sharing.

“Currently, around 16 zettabytes of data are produced per year and for the year 2025, 163 zettabytes of data are expected.” In its early stages, the internet was only considered as a source of information with websites like Wikipedia, but this understanding was shifted into becoming a tool for communication and data sharing.

Governments used to collect data on their citizens even before the internet era in the form of written surveys which can be archived and monitored in order to protect the system and the institutions by minimizing credit default rates, linking the

establishment of infrastructure to demographic evolution and collecting taxes based on income but this process was highly time and cost consuming.

This large amount of constantly updated near real time data became a vital instrument for researchers and analysts providing predictions and advanced insights on public issues such as unemployment in a better accurate methodology than standard government reports.

Social data being shared includes information about medical status, dating preferences, personal thoughts and real-time location.

1.2.Types of social data:

Four identifiable types of social data: words, locations, nature, and behavior.

- Words: huge amount of internet content is in text format provided by user interaction using posts, comments and search engines. Furthermore we identify two types of statistical information being shared online through a probability survey or a census and through public records such as income tax, credit card or any other financial or commercial transaction records, unemployment, and payroll.
- Location: data on pinpointed location and related movements is being provided by technologies such as Global Positioning System (GPS), location based applications, and location based gaming etc.
- Nature: generated data on natural or biological processes falls under the category of “nature data” which includes sensory data like the weather, temperature and bacterial spreads.
- Behavior: researchers and analysts study users’ behavior on multiplayer online games such as Farmville and Call of Duty.

1.3.Social data and the business sector:

The appearance of individual digital identity (individual data available through electronic devices) is being used by businesses and organizations to enhance products and services by making production cost efficient and by targeting specific segments of audiences or consumers based on their desires and expectations.

Social networking sites are selling user data to business companies and other third parties in order to attain a deeper understanding of their clients through “data mining” improving decision making processes and marketing strategies within the businesses.

Alongside businesses and corporations use of available consumers data, consumers themselves are using other consumers data on shopping experiences in their decision making process to purchase products and services.

Social networking services were the main source of this data generation but with technological advances allowing the creation of daily life devices including smartphones, smart watches and music devices that can also collect user data, the amount of personal data generated increased substantially.

Businesses can also use social data to detect if different marketing techniques such as shelf organization process with malls and supermarkets, and previous customer purchases can affect consumer decision making process.

When a user approves the privacy policy of most social networking services, they approve sharing their personal data with third parties.

Collected data may include demographic information, social media preferences, shopping experiences and more which can be used for better product personalization and to extract consumer’s behavioral patterns.

1.4.Computational social science:

The concept allows the use of social data for research purposes by combining computer and networking science with social sciences. In the beginnings, scientists relied on individual interviews to collect and analyze data, thus, being limited to restricted view of social information obtained with little accuracy and time/cost consumption, but with the rise of social data and technological advancements, scientists were able to collect huge amount of social data generated by electronic devices and social networking sites swiftly and cost efficiently on any targeted segment of audience subject to study. With the huge amount of social data being shared, scientists are being able to have a wider view of information. Scientists are using social networks and cell phone data that allow them to collect even more information than before in order to conduct online experiments.

1.5. Social data analytics:

Social data analytics is the process of understanding insights on human interaction within social contexts, often relying on data generated from social networking sites. The objective may be to reach a deeper understanding of human behavior or to infuse a certain message to a targeted audience.

Social data analytics include two major steps. First, collecting data from social networking platforms and secondly, analyzing the collected data which requires updated data analysis. Other factors may also be required to achieve an accurate analysis of the data such as understanding the contextual aspects of the data, relevance, as well as the data time frame. To summarize, social data analytics is done via data mining techniques with the purpose of extracting insights from the analyzed data.

Social scientists are provided with a human trace through social data analytics which can be used in sectors such as politics, sociology and geology.

Political scientists are able to use social data analytics to examine and analyze protests being live streamed through Facebook and other social networking services all around the world, furthermore, they are able to observe exchanges between communities using different languages.

1.6.Obtaining social data:

With the development of web 2.0, social networking services became popular providing application programming interface (API) which allows two or more applications to communicate with each other, thus providing access to social networking services data by responding to user's queries.

Sources of social data primarily include Facebook, Twitter, Snapchat, Tinder, Wikipedia, and others. Many of these services, in the attempt to preserve user privacy, don't allow third parties which do not possess required access permissions to access their data. Furthermore, many of these social networking services require a fee from third parties like Analysts, businesses and corporations in order to obtain the data.

Social data analysis comprises three operations:

- "Data identification."
- "Data analysis."
- "Information interpretation."

To maximize the results, analysts ask relatable questions according to the user in order to reach a desired answer.

In an attempt to reach the suitable questions associated in determining the right data sources affecting the nature of the data analysis, the important queries to be asked are: who? What? Where? When? Why? And how?

Chapter two

Privacy concerns and related platforms

2.1. Introduction:

Determining the accountability of user privacy violations or poor privacy settings given by social networks is rising with no concrete answer nowadays, especially that a more effectively regulated application programming interface (API), might cause applications to abort certain tools, such as third party purchase of user data, generating a big portion of the applications cash flow on a yearly basis.

Privacy concerns on social media relate to techniques of data protection allowing user control over the online display of personal information, the right of mandating personal privacy, data storing and repurposing, user data acquisition by third parties and so on.

The amount of social information becoming huge online and stored in the cloud, the problematic of online user privacy has increasingly transformed into a concern putting the ability of the cloud platform to maintain user privacy into question.

After social profiling became a reality, privacy concerns online became increasingly serious especially when social networks like Facebook and MySpace collect all social interactions happening on their platforms and store them for future use.

Potential dangers include third party personal information disclosure, cyberstalking, location disclosure, social profiling and authorities' use of social networking services for investigations without the requirement of a warrant.

Privacy concerns are due to the large volume of information being shared on social networks and processed each day.

Furthermore, the technologies used in the framework of many social media applications may intrude user privacy.

Since the beginning of the digital era with the creation of web 2.0 in the 2000s, social media applications have grown increasingly, and notorious platforms became Facebook, Twitter, Instagram, and Snapchat from the mid-2010s.

Application features allowing users to interact publicly in photos, videos, messages, invitations... are the main source of third party access to online personal information.

The cloud platform and the scale of user data access by other users and social networking services, generated hot topics of ethical consideration and legality.

2.2. Causes of online privacy concerns:

2.2.1. Overlook:

Several causes for online privacy invasion can be identified throughout social networking services as it is recognized that by design, social media applications interfere with the control of access to user generated data since its sharing on social media platforms is crucial to their function.

One reason for this is that legal frameworks around the world are absent or rather do not provide the appropriate mechanism for protecting users who share their data online from having their interactions and posts shared beyond than they intend.

Even with privacy settings, there is no guarantee that the cloud platform or any other platform are able to maintain privacy of private user information beyond the limited audience (friends or followers) set by the user.

Social media applications companies actually need private user information to become public in order for them to operate.

2.2.2. Offering multiple levels of privacy:

The privacy policies of social networking services vary in the scope of information required from users to provide for opening an account and/or using the platform.

Facebook requires users to provide information about their name, birthday, phone number and address, other applications require in addition information about interests, hobbies and relationship status.

Nevertheless, social networking services like Mtch.com allow their users to surf their platforms anonymously thus protecting data privacy in full

2.2.3. Public behavior concern:

Even after realizing the potential dangers of publically sharing personal identifiable information on social media platforms, users are still not caring to have a look on privacy policies, nor they are making the effort of adjusting the terms to their required level of privacy, and one explanation for that is that many users prefer to enjoy the features presented by social media platforms, being up to data on social activities, bragging about what they do to their friends... as long as the features presented are free of charge which creates what is known as “the privacy paradox”.

Users that are manifesting privacy concerns on social networking services but won't examine and alter their privacy settings to their convenience constitute what's called “the privacy paradox”.

It has been noted that for sites that do encourage their users to share their personal information publically, most of online users have no problem with openness to share their private information to a significant scale of audience.

A Boston consulting group research have shown that “personal data privacy is a top issue for 76% of global consumers and 83% of U.S. consumers.”

2.2.4. User awareness in social networking services:

The kind of trust users are having with social networking services is defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party." A majority of users are exposing their phone number, current address, and more importantly checking-in with primarily Facebook exposing their pinpointed location without realizing the consequences of sharing these information.

Social networking users are the main source of targeted information online since they leave digital imprints whenever they surf on browsers and social media applications, taking into consideration that users are trusting social networking services. This is very concerning especially that the public is not questioning the privacy policies adopted by social networking services, there is some sort of blind trust with online service providers that might escalate to a total disregard of resulting privacy risks, furthermore, the concern persists since identifiable personal information are being provided to third parties via certain tools and applications and APIs structures are enabling users to extract these information if they have the knowledge to do that.

Therefore, there is a need to raise awareness among social media users in order to face challenges of privacy resulting from mere user unawareness, this can be achieved by appealing to social networking services themselves to educate their clients (users) on the dangers of recklessly sharing critical private information.

2.3. Data access methods:

2.3.1. Data sharing with third parties:

Taking Facebook as an example, almost all famous applications therein (such as FarmVille) share user information with third parties including tracking and advertising companies, although Facebook privacy settings clearly states they can provide third parties with "any of the non-personally identifiable attributes we have collected", they are

violating it. If a user clicks on a certain advertisement, Facebook will provide the link address to advertising companies containing a direct link to the user's profile.

“Take With Me Learning” was an application owned by a company that is prominent with collecting and storing student's data in order to provide them with survey and advertising companies for a service fee depending on the amount and the quality of the data.

The application requires a set of personal information including the user's name, school name, age, and e-mail address.

2.3.2. Application programming interfaces (APIs):

APIs collect personal information in masse and the privacy debate is related to the difficulty of assigning a specific information to a specific user, however the Facebook and Cambridge Analytica Ltd incident raised red flags concerning APIs since Facebook allowed a political consulting firm to build an online platform with the only objective of data collection.

APIs can collect, store and share data that is not publically accessible which results in privacy concerns over the capability of these platform to manage and maintain private information but it also presents huge opportunities for researchers to attain efficient and precise results.

APIs are a set of algorithms, protocols and routines allowing to build software applications, simplifying sharing data between communities and applications by using query language and limiting external program access to a certain set of features.

The problem was when Cambridge Analytica Ltd was able to take advantage of a loophole in the system in order to collect data not only on the people using the application but also on their friends without acquiring an informed consent from them.

2.3.3. Search engines:

Search engines allow the browser to experience a platform whereby entering certain key words in a search box results in a list of potentially targeted websites ready to explore rather than checking each website separately.

Many search engines available online may conduct the user to undesired or deceptive sites where he can have access to personally identifiable information or are filled with viral programs that can seize his own personal information in order to share it for benefit.

On the other hand, search engines like DuckDuckGo are very serious about user privacy and will not tolerate any violation upon data privacy.

2.3.4. Location data:

Most social media applications gather information about the geo-location of their users either voluntarily (using voluntary check-ins by users through applications like Facebook Places and Foursquare), or by the applications themselves using technologies such as cell phone network triangulation, IP address geolocation,.. In the second approach where the user's geo-location is shared by applications, users are sharing content such as texts, photos or videos with the location where the content is produced implicitly. Furthermore, online platforms such as social media add –implicitly - to the location other forms of information such as capture time for photos and videos, device type, and OS language associated with the content shared by users.

2.4.Potential dangers:

2.4.1. Identity theft:

The information extracted from users Facebook profile pages that could assist with identity theft include: Full name including middle name, hometown, date of birth, residential information, relationship status, and other interests or hobbies.

In fact, a study in 2009, provides that “it is possible to predict an individual's most or all 9-digits social security number, based on data shared online through social networking services.”

Bogomil Shopov (IT consultant), said that “he has purchased personal information related to more than one million Facebook users for the surprisingly low price of USD 5.00.” The purchased data included users’ full name, links to their Facebook profiles, and e-mail address.

Situations have been reported where malicious attacks on users are ending with extracting photographs, thus facilitating “Identity theft”.

Cases of stolen media content (photos/videos) from users online in order to facilitate “identity theft”, have been reported.

It has been advised that individuals do not share their social security number on social networking services and if they insist, they should hide it from “friends” or “followers” they don’t personally know.

Since the volume of generated data online is immense, it is not difficult to deduce other information like the user’s social security number.

Furthermore, users on social networking services are not taking full action to shield themselves from identity theft.

2.4.2. Preteens and early teenagers:

This is of high concern since early teenagers are not a well-educated segment of society on public social networking platforms, as well as shielding themselves online, and the results that might occur while sharing too much personal information publically.

Society applies pressure on preteens and early teenagers which encourages them to disclose private information online including activities they are doing, sharing current location, sharing their thoughts and opinions, and exposing who they spend time with.

Rising concerns from parents and teachers and working on increasing adolescent’s concern towards online privacy issue will contribute to impact users behavior towards

online privacy, thus awareness in society becomes crucial in order to acknowledge the level of importance related to online privacy.

Preteens and early teenagers are the most vulnerable age segment when it comes to private information sharing on social networking services.

As the number of teenagers engaging in social networking sites is increasing, they believe they can share whatever is on their mind to the public without realizing the potential harms of sacrificing their own privacy.

Adolescents share private information online to keep up in an up to date manner with their peers who are practicing these sharing behaviors.

2.4.3. Sexual predators:

Many notorious social networking services are trying hard to promote their platforms as safe for interactions between users, but due to the large amounts of data being shared and the fact that hiding under a pseudo-identity is possible, such services are becoming increasingly susceptible to sexual attacks.

Widely publicized cases have shown the threat imposed on users, one of them is the case of Peter Chapman who succeed in adding over 3,000 friends on Facebook under a false name and engaged in raping and murdering a girl (seventeen years old) in 2009.

Furthermore, we present the case of Evergreen girl (twelve years old), who was found unharmed by the Federal Board of Investigations using Facebook as a result of her mother knowing of a conversation she had with a man through the notorious social networking application. More and more online sexual predators are being exposed currently reaching a weekly basis.

2.4.4. Stalking:

Social networking services are making it easier to build a network of acquaintances with whom a user can share his videos, photos, locations, contact information and interests

without the need to actually meet them, thus the probability for stalking users online has been well noted.

High concerns have been noted with applications allowing the ease of access to private messages and e-mails on social networking services, and if a user's phone is stolen or missing, anyone is capable of accessing these private conversations.

Carnegie Mellon University conducted a study on Facebook profiles of their student revealing that "800 profiles mentioned current address and at least two classes they are enrolled in, practically giving information on their precise location at a precise time."

Facebook places is one of the most concerning location based Facebook service that allows users to publically share their locations to the networking community.

Some online applications has make it possible for users to add others without their knowledge, thus allowing them to track when a user is online.

With the large scale of information being posted online, the potential of stalking users is increasing without them being aware of the fact.

Furthermore, some smartphones are embedding the coordinates (longitude and latitude) of a captured photo and send it directly to the application allowing to track the pinpointed geo-location of a user at capture time.

2.4.5. Unintentional fame:

Media content can be embarrassing, thus gaining unintentional fame over embarrassing content may affect a person's reputation, employment chances, character, and relationships... to end up with infringing an individual's right to the pursuit of happiness.

High profile embarrassing incidents have occurred raising privacy concerns, highlighting the ability of private information to be rapidly shared on social networking services publically.

Unintentional fame is a result of sharing media on social networking services of individuals - without their knowledge - that goes viral between the users.

Consequently, users should have the right to remove their information from media content that was shared publically, this right is a legal concept called "the right to be forgotten".

However, in the United States, the contradiction between the "right to be forgotten" and protecting freedom of speech guaranteed in the first amendment of the US Constitution is still a matter of debate.

Application of the "right to be forgotten" is identified in many jurisdictions such as Argentina and the European Union, nevertheless we have identified cases on the state level in the US where the "right to be forgotten" is recognized.

A lot of cases with unintentional fame have lead affected individuals to undertake legal action.

2.4.6. Job market and workplace discrimination:

Employers are actually hiring third party companies to monitor their staff online on their behalf in order to ensure that employees are not leaking sensitive information that could damage the reputation of the company on social networking sites.

Privacy concerns and monitoring of online social profiles is not limited to prospective employees but also targets current staff where many cases have been noticed of employees

being sacked for sharing online downgrading information about their current employers or colleagues.

An opinion by Workforce.com stated that employers who use Facebook or MySpace for the purposes mentioned above could face legal action: A potential employer could be charged with discrimination if he or she relies on social networking services to screen a job applicant and refuse his or her application based on what they see.

While it's not predicted that employers will continue to rely on social networking services to monitor their staff and to screen job applicants, it is noted that this course of action might be considered illegal under many jurisdictions.

We were unable to find any federal law that prohibits employers from monitoring their staff and prospective employees on social networking services.

CareerBuilder.com estimates that "as of 2008, one in five employers rely on social networking services to screen potential job candidates increasing from only 11% in 2006."

However, 24% of managers stated that they hired job candidates based on their profiles on social networking services and suggesting that an individual's online profile can be used positively.

Moreover, monitoring staff's usage of social networking sites is adopted to make sure that employees are not wasting time during working hours.

2.4.7. Online victimization:

Estimates show that "approximately 9% of online victimization is being on social networking sites and that the majority of victims are women who have been sexually offended over social media applications."

However, some users engage in bad social behaviors online which can affect negatively the online experience of other users which created a significant scale of online inter-user victimization.

Negative social behavior over the internet such as sexual content discussions and aggressive attitudes increases the will of offenders to achieve what they want in real life.

2.4.8. Commercial tracking:

Every activity or transaction online is leaving behind a cyber-footprint and researchers' usage of these footprints is increasingly raising ethical and privacy concerns along the way since huge amount of online shared data is collected by private corporations such as Microsoft, Google, Twitter and Facebook giving new understandings of everyday life.

Social networking services users are not aware of the scale of their audiences since shared information is not being received only by followers and friends and data is being collected just by searching something like "favorite night club" on search engines.

In 2010, the Wall Street Journal conducted an investigation revealing that "many of the Facebook applications are sharing user identifying information as well as their friends to advertising and tracking companies in violation of the Facebook privacy policy."

The investigation studied 10 of Facebook most notorious applications including, Farmville with 56 million gamers, Mafia war with 22 million gamers and revealed that these applications are sharing users ID with data aggregators.

It is appealing to the public that a worldwide communication system model is established through networking services over the internet, but private companies constituting market forces are controlling access to such powerful resource.

2.4.9. Surveillance:

The Department of Homeland Security (DHS) was authorized starting October 18, 2017 to use personal information generated on social networking services to screen immigrants coming to the United States.

In September 2017, The DHS made this authorization public in the Federal Register stating that “social media handles, aliases, associated identifiable information and search results will be added to an immigration applicant’s file.”

The DHS came back in late September 2017 by saying that there is nothing new concerning the use of social media as an investigative tool with one of the departments’ spokesman declaring that the DHS has been relying on social networking services for intelligence for years.

Social Media Monitoring Software (SMMS) is being used by Governments to track users as they communicate elaborating charts on associations, acquaintances and relationships.

SMMS like Geofeedia, Dunami, XI social discovery, Dataminr, and SocipoSpyder are increasingly becoming a demanded product purchased by federal agencies, law enforcement, defense contractors, politicians, fortune 500 companies and the military.

It is to be noted that acquiring information by authorities about users which is not publically shared requires a subpoena, public pages and profiles on applications like MySpace and Facebook became an important intelligence asset for law enforcement.

The Federal Bureau of Investigation (FBI), has assigned undercover agents on several social media applications.

Recently, law enforcement agencies on the state level began to consider social networking applications as a valuable resource.

2.4.10. Invasive privacy agreements:

The ethical problem exists because according to privacy policy agreements by social networking services, the private information generated on their platforms is strictly accessible and managed by the sites private operating systems, increasing the moral obligation for social networking services to ensure user privacy within their operating systems.

Another issue of privacy is the social networking services privacy agreements in which social networks state that they own all content shared by users on their platforms including photos, videos and messages collected and stored in their databases even after deleting an account.

In addition, another main concern is that social media applications have lengthy privacy policies that are not very easy to read or understand and that they are placing the terms affecting users personal data privacy at the end of the privacy policy assuming users will not have the time to read them fully.

2.5.Social networking platforms:

2.5.1. Facebook:

Mark Zuckerberg, Facebook CEO, launched the application in 2004 targeting university students and only users with “.edu” e-mail address could sign-up for an account.

In time, Facebook allowed users who are not university faculty or students, and those who do not share a common network to join the platform thus becoming more public.

Facebook was out under the microscope for arising privacy issues concerning the constant change in privacy settings policy over time as well as for the Facebook applications.

Facebook updated users’ profile model allowing users who are not friends to see other users’ personal information on their profiles despite being set as private.

Requiring permissions to access certain information never clarified why this information is needed by social networking services. Hundreds of complaints on Facebook’s privacy settings have been sent to the application with one of them claiming that “Facebook is relentlessly trying to oblige thousands of users that they spent years trying to attract into sharing more personal information publically through the platform.”

Facebook allowed, as of January 18, 2011, third party users’ access to address and phone number information, but it still allows access to less precise personal information such as employment and hometown.

However, user complaints continued to accumulate claiming that “the new privacy settings were too broad, confusing and aiming to increase shared information by users.”

2.5.2. *Instagram:*

Instagram tracks the location of photos shared by users on the platform even if they don't geo-tag them, thus anyone can view the exact capture location of an uploaded photo. This is alarming because users usually upload photos from places they frequent or even from their current residence address.

The search function on Instagram includes searches on people, tags, and places that allow the inspection of any location globally to search a vacation venue, discover the interior of a restaurant, and even to experience a location without ever being personally there. The impact is that corporations and people are gaining more access in real-time to every location on earth including the culture as well as people's private lives.

Furthermore, what's concerning is that when users search the platform using these features for a precise location, Instagram shows the personal individual photos of users captured and uploaded as well as all the “likes” and “comments” presented on the uploaded photos to that precise location even if the account is set as private.

2.5.3. *Twitter:*

When a Twitter user consents to its privacy policy, he approves “the collection, storage, transfer, manipulation, disclosure, and other uses to information generated through applications, websites, APIs, SMS, and other third parties.”

Twitter software systems automatically store information such as browser type, visited pages, IP address, cell phone vessel... Account denominators (IP address, username...) allowing the identification of the user will be deleted after 18 months.

Twitter is a platform where users are allowed to share photo, video and text content with their “followers”. Messages can appear before any “Twitter account user” if the user does

not adjust the default privacy policy. On the user public timeline, the last 20 “tweets” are displayed.

A court order in January 2011, obliged Twitter to provide information about private accounts related to the WikiLeaks cases. Twitter responded by stating that: “users should be notified and given time to defend their constitutional rights, related to the First Amendment of the Constitution, in court before their rights are compromised.”

Another privacy concern with twitter is that “tweets” are accompanied with location information when a user shares them and most users are sharing their tweets not knowing that they are sharing along their location information.

Twitter users can simply avoid the disclosure of their location by disabling location services on the privacy settings.

2.5.4. Snapchat:

Privacy concerns started with Snapchat with a new feature introduced in the new update in 2017 called “Snap Maps” which allows any Snapchat account holder to track someone’s location activity unless the user restricts this visibility through the privacy settings to all of their friends, a selected group of friends or no one at all which the application call “ghost mode”.

Snapchat privacy policy stated that: “Snapchat only collects phone number, e-mail address and Facebook ID in order to better connect the user to find friends.” If a user uses his phone number to find friends and he owns an IOS device, twitter is able to retain all the information contained on that device’s contact list including names and phone numbers.

Users are allowed to do “Live stories” starting 2015 when a new update of the application was introduced, it allows users to generate a collection of crowdsourced media (photos/videos) in snaps related to a specific event or location.

Snapchat has another feature called “stories” which allows users to send photos into a story viewed by friends as much as they want until it disappears after 24 hours.

Snapchat also transferred contact and location information to its analytics service provider without user consent and without mentioning the ability to do that in the privacy policy.

2.6. The Facebook and Cambridge Analytica case:

2.6.1. Facts and process:

Cambridge Analytica (hereafter “the company”) is an English political consulting firm, who collected, stored and processed data for the purpose of giving consultancies to concerned parties in electoral processes.

Conservative business man Steve Bannon and Robert Mercer cofounded the company, which was incorporated in January 2015 with Alexander James Ashburner Nix appointed as director and chief executive officer.

In 2013, the company was a subsidiary company of the SCL group and in consequence of the Facebook and Cambridge Analytica incident, the business ended operations in 2018.

An application called “This Is Your Digital Life” was established by Alexander Kogan who shared the collected data of users with the company.

The company established a survey on Facebook in which it acquired an informed consent from users in order for the survey to be conducted, however the collected information on “This Is Your Digital Life” didn’t only contained data about Facebook users who consented to the survey but also the data of all of their friends exploiting a loophole in the Facebook system.

That was the process of the collection of millions of users’ private data on Facebook by Cambridge Analytica.

In December 2015, Harry Davies of The Guardian first reported the collection of data from millions of Facebook users by the company with regards to Senator Ted Cruz’s political campaign.

2.6.2. Impact and responses:

2.6.2.1.Facebook:

Facebook CEO, Mark Zuckerberg stated that the application will adopt measures and safeguards to protect the personal data of users which resulted in the implementation of the GDPR requirements in Facebook activities worldwide and the creation of a “clear history” tool that allows users to delete their data on the application conforming to “the right to be forgotten”.

As a result of the scandal, Facebook shares value dropped dramatically resulting in significant losses.

2.6.2.2.Cambridge Analytica:

The group's London-based affiliate, SCL Elections Ltd, has received a legal warning asking them to provide all the collected data in their possession and related to American professor David Carroll, US-based voter, professor of multimedia design at the Parsons School of Design in New York.

Furthermore, the Office of the Information Commissioner of the United Kingdom announced, In early July 2018, its intention to fine Facebook £ 500,000 (\$ 663,000), stating that Facebook violated the law by not protecting users information.

Alexander Kogan stated that at the time he did not know what he was doing and that he is now convinced that basic concept of "Everyone knows nobody cares " which the company adopted was faulty.

2.6.2.3.Governments:

India and Brazil required the company to report on how the collected data was used in political processes within their jurisdictions.

Canadian Facebook users were less affected by the scandal than US users, they were still not spared according to the CBC report stating that “data from approximately 600,000 Canadians had been collected by Cambridge Analytica.”

The Canadian House of Commons finalized a formal inquiry into the matter.

The Privacy Commissioner of Canada, demanded stricter regulation for the data protection of Canadians, furthermore, he required that his agency be provided with the prerogatives to execute orders and apply penalties.

The government of Papa New Guinea closed the application for a month in order to study the advantages and disadvantages of Facebook with matters related to pornography and fake accounts.

The British Parliament discussed the case with Facebook CEO Mark Zuckerberg but wasn't satisfied with his answers.

2.6.2.4. The public in general:

The case was nevertheless important because it initiated an international debate on ethical and technical standards to protect data privacy.

Activists on consumer right protection demanded protection for consumers on social media applications with regards to personal data privacy and fake news.

In the United States, Facebook was challenged before the court system by numerous citizens claiming infringement and misuse of their personal data without their consent.

2.7. Facebook testimony to US Congress:

Before the congressional hearings started, the expectations were that Zuckerberg is going to be grilled by the Senate since the rare Washington appearance comes as Facebook's CEO Company faces many questions about data privacy and its broader role in American life.

Zuckerberg's testimony before "the United States Senate Committee on Commerce, Science and Transportation" began on April 10, 2018.

The committee investigated Zuckerberg on the processing of data with regards to Cambridge Analytica,

Zuckerberg stated that among the 87 million Facebook users affected by the scandal, his own personal account was subject to data collection by Cambridge Analytica.

The testimony kept a lot of questions unanswered but clearly demonstrated that US legislators do not have the knowledge nor the firm intent to regulate on data protection and privacy, and certainly they are unable to force a notorious multi-billion making company like Facebook to make adjustments to their business model.

In deduction, several senators asked appropriate questions targeting the heart of the data privacy issue, but we can easily say that Senate's tech illiteracy saved Mark Zuckerberg.

Furthermore, we have collected nine of the most ridiculous questions asked by the US Congress to Mark Zuckerberg as follow:

1. "Is Twitter the same as what you do?"
2. "If I'm emailing within WhatsApp ... does that inform your advertisers?"
3. "How do you sustain a business model in which users don't pay for your service?"
4. "What was Facemash, and is it still up and running?"
5. "What if I don't want to receive ads for chocolate?"

6. "My son is dedicated to Instagram, so he'd want to be sure I mentioned him while I was here with you."

7. "Would you bring some fiber, because we don't have connectivity?"

8. "Some people refer to Peter Thiel's startup, Palantir as Stanford Analytica. Do you agree?"

9. "Did you know that the Motion Picture Association of America is having problems with piracy and ... this is challenging their existence?"

In conclusion, experts stated after the hearings that "Congress could have been a lot harder for Zuckerberg if its members were better informed about the functioning of social networks and the Internet." If that was the case, interrogating Zuckerberg would have been a lot more serious pressuring on the right concepts of data protection that needed to be addressed.

Chapter three

Social data privacy laws: a global comparative approach

3.1. The United States of America:

3.1.1. *Relevant legal framework today:*

We are not aware of any Act issued by the US Congress directly regulating social data privacy, thus tech companies are currently self-regulating the sector similar to the case of US banking and financial sector prior to the financial crisis of 2008. Nevertheless, the only federal law issued by the US Congress and still in effect, that can be referred to as regulating to a certain extent some aspects of social data privacy including data generated on social media is the Privacy Act of 1974.

3.1.1.1. *The Privacy Act of 1974:*

Enacted in December 31, 1974 by the US Congress, the Privacy Act of 1974 provides for “minimum standards of fair data practices that governs the collection, storage, management and termination of personally identifiable information to be stored in a federal registry system by assigned federal agencies.”

The Act defines a record system as “a group of records under the control of an agency from which information is retrieved by the name of the individual or by an identifier assigned to the individual” requiring governmental bodies to inform the public of their registry systems by publishing them in the “Federal Register”.

The Act prohibits: “the disclosure of information contained in a registry system without the written consent of the concerned individual or data subject”, unless the reason for disclosure falls within the boundaries of twelve exceptions explicitly cited in the Act.

The Act allows data subjects the access to their records and the right to modify or update the information therein, furthermore it sets out requirements and limitations for federal agencies concerning the retention of various documents. In addition, the Act allows data

subjects to be informed on whether their information has been disclosed to a third party of any kind.

3.1.1.1.1. Conditions of disclosure:

The privacy Act of 1974 states in part:

"No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."

This statement doesn't limit the scope of the nature of communication allowing to include written, oral, electronic or mechanical communication, furthermore it demands "the written consent of the data subject" to disclose such information, nevertheless, the burden of proof is on the data subject to prove that an "unlawful disclosure" or any disclosure had actually happened.

Thus, social networking sites like Facebook are required to obtain an approval from the user on an authorization request to disclose information to third parties.

Despite that the Act limits the infringement of personal data through disclosing to third parties, it enumerates twelve exceptions making that kind of disclosure eligible as follow:

- "For members of an agency who need such information in the performance of their duties."
- "If the Freedom of Information Act requires such information."
- "If the information that is disclosed is compatible with the purpose for which it was collected."
- "If the Bureau of Census needs such information to complete a particular census."
- "If the third party explicitly informs the individual that the information collected will serve only as a form of statistical research and is not individually identifiable."
- "If it is historically relevant to be added to the National Archives and Records Administration."
- "If such information was requested by a law enforcement agency."
- "If such information is deemed beneficial to the health or safety of an individual."

- “If such information is requested by the House of Congress or by one of its subcommittees.”
- “If such information is requested by the head of the Government Accountability Office or by one of his authorized representatives”.
- “If such information is requested through a court order.”
- “If such information is requested through the Debt Collection Act.”

The Act obliges US federal agencies to set out administrative and technical safeguards in order to anticipate “unauthorized disclosure of personal records.”

In order to protect individual privacy, agencies are required to specify the authority no matter what is the source (Act, Statute, Executive Order...) that approves the solicitation of personal records, as well as indicating whether this disclosure is voluntary or mandatory. This disclaimer is present on all federal governmental forms seeking to retain personal information from individuals.

3.1.1.1.2. Department of Justice:

In Subsection U of the Act, there is a requirement for every federal agency to establish a “data integrity board” which submits to the “Office of Management and Budget” an annual report that includes all complaints of data breaches and violations of the Act like the use and sharing of information for an unauthorized reason by the Law or the holding of information in violation of the First Amendment of the US Constitution as well as reporting any corrective action undertaken

3.1.1.1.3. Computer Matching and Privacy Protection Act:

This Act is an amendment the privacy Act of 1974 establishing protection to data retained in automated programs.

Safeguards were establish in order to ensure:

- “Uniformity of procedures in the execution of matching programs.”
- “Due process for subjects to protect their rights.”
- “Monitoring matching programs by setting up data integrity boards in each agency that engage in matching to monitor the agency's matching activities.”

3.1.1.1.4. Access to records:

The Privacy Act also states:

“Each agency that maintains a system of records shall...”

- “Upon request by any individual ... permit him ... to review the record and have a copy made of all or any portion thereof in a form comprehensible to him ...”
- “Permit the individual to request amendment of a record pertaining to him ...”

The Act affects every individual defined in the Act as "a US citizen or legally lawful foreign national for permanent residence".

The Act is applicable only on data collected and stored by agencies, therefore, any public or governmental body which is not an agency is not subjected to the mentioned Act.

US President Donald J. Trump issued an executive order entitled “Enhancing Public Safety” on January 25, 2017 excluding the application of safeguards set out by the Privacy Act to records retained on Aliens who are not defined as US citizens or holders of a permanent residence “to the extent consistent with applicable law.”

3.1.1.2. Several attempts of regulation:

The US Congress tried and still trying to pass several bills in order to regulate the social data privacy sector but lobbyists of the tech companies have fiercely fought and still fighting against any federal legislation regulating any aspect of the sector. From those attempts we mention:

3.1.1.2.1. Child Online Protection Act (COPA):

Promulgated in 1998 by the US Congress for the purpose of “preventing minors from accessing dangerous material on the internet.”

The main application of the Act was to mitigate identity theft among children surfing the internet.

This Act was aimed by lawmakers to regulate pornography in partial correlation with the “Communications Decency Act” deemed unconstitutional in 1997 by the US Supreme Court.

Three lawsuits before the American federal court system resulted in a permanent injunction of the Act by The US Supreme Court in 2009.

3.1.1.2.2. Social Networking Online Protection Act:

Introduced to US Congress in 27/04/2012, by New York Congressman Eliot Engel, this Act prevents employers from:

- “Requiring or requesting an employee or job applicant to provide a username, password or other means to access a private email account or personal account on a social network website”;
- “Dismissing, disciplining, discriminating against, and refusing employment or promotion to an employee or a job applicant who refuses to provide such information, filing a complaint or instituting proceedings under this Act, or testifying to such proceedings.”

Inflicts, consequently to breaches of this Act by an employer:

- “Civil penalties”;
- “The power of the secretary of labor to bring actions in injunction”;
- “The jurisdiction of US District Courts to provide legal or equitable relief, including employment, reinstatement, promotion and payment of lost wages and benefits.”

Amending the “Higher Education Act of 1965” and the “Elementary and Secondary Act of 1965”, the acts prohibits educational institutions from requiring student or prospective students to provide user account information such as passwords.

The Act “prohibits admission denials, suspensions, expulsions and any other disciplinary or discriminatory action against students who refuse to provide such information, to file a complaint, to institute proceedings or to testify in related proceedings.”

This bill died in a previous Congress, thus it was never enacted.

3.1.1.2.3. Password Protection Act of 2012:

Introduced to US Congress in 09/05/2012, by New Mexico Congressman Martin Heinrich, and emending the federal criminal code, this Act requires a fine on any employer who, knowingly and intentionally:

- “Obliges or compels any person to provide the employer with a password or similar information to access a protected computer that does not belong to that employer”;
- “Discharge, discipline, discriminate or threaten to take such action against any person who does not authorize access to this computer, has filed a proceeding, or has testified or is about to testify in such a course.”

The Act states that “nothing in this Act shall be interpreted as limiting the power of a court of competent jurisdiction to decide on an equitable basis in a civil action, if it considers that the information sought is relevant to the protection of intellectual property, a trade secret, or confidential business information of the party seeking redress.”

The Act discharges an employer from this limitation if:

- (1) “The employer discharges or disciplines an individual for a just cause”;
- (2) “A state adopts a law that expressly waives such a prohibition with respect to a particular class of government employees or agencies, and the employer's action relates to an employee of that class”;
- (3) “An executive agency, military department or other entity of an executive branch expressly waives the prohibition against a particular category of employees who may have access to classified information”.

This bill died in a previous Congress, thus it was never enacted.

3.1.1.2.4. Social Media Privacy Protection and Consumer Rights Act of 2019:

Introduced to Congress in 17/01/2019, by sponsor Amy Klobuchar senior senator for Minnesota, this Act sets requirements for operators of the online platform “to inform a user, before creating an account or using the platform, that the user's personal data generated during the online behavior will be collected and used by the operator and third parties”. “The operator must provide the user with the ability to specify privacy preferences.” Furthermore, “An operator may refuse to provide certain features or full access to a user if the user's privacy options disable the platform from operating.”

The operator must:

- “Offer the user a copy of the user's personal data that the operator has processed, free of charge and in an electronic format”;
- “Notify a user within 72 hours after learning that their data has been transmitted in violation of the security platform.”

An infringement of the privacy requirements upheld by the Act must be considered “an act or practice that is unjust or misleading under the Federal Trade Commission Act”.

Governmental bodies subject to the Communications Act of 1934 can be subject to application of this Act by the Federal Trade Commission.

Currently, public bodies governed by this law are exempted from the monitoring of the FTC, and solely non-profit organizations are subjected to this monitoring “if they bring substantial economic benefits to their for-profit members”.

Breaches of this Act may be subject to a civil case by a State or a Federal court.

This bill will be considered by the adequate US congressional committees.

3.1.1.2.5. Social Media Use in Clearance Investigations Act:

Introduced to US Congress in 07/02/2019, by Massachusetts Congressman Stephen Lynch, the Act requires the Office of Management and Budget “to report on the examination of social media activity during security clearance investigations.”

The House of Representatives approved this bill on February 11, 2019 and it will be transferred to the Senate for discussions.

3.1.1.2.6. Data Privacy Act:

Introduced to Congress in 27/02/2019, by sponsor Catherine Cortez Masto, senior senator for Nevada,

The Data Privacy Act also called “the Digital Accountability and Transparency to Advance (DATA) privacy Act enhances the safeguards of data privacy for US consumers, while making sure that businesses focus on implementing new data security standards and crucial privacy protections. This legislation also strengthens “research on technologies that protect the privacy of Americans and protects small businesses from unnecessary regulation.”

This legislation undertakes an active approach to protect consumer data by ensuring that Americans have a say on how their data is used. This bill requires companies to prioritize data protection and transparency, while obliging US Congress and US government agencies to strengthen and make consumer data confidential across the United States a priority.

The Data Privacy Act requires corporations “to provide users with reasonable access to a method of opt-out.”

This legislation requires that three simple standards be applied to the collection, management, storage and sharing of data:

(1) “Reasonable: Must be linked to a legitimate business or operational purpose, which is contextual and does not subject an individual to unreasonable privacy risk.”

(2) “Fair: Data practices cannot discriminate between protected features, including political and religious beliefs.”

(3) “Frank: companies cannot engage in deceptive data practices.”

The bill requires prior approval in two situations:

(1) “Collection or disclosure of sensitive data such as genetic, biometric or location-specific data.”

(2) “Disclosure of data outside the parameters of the relationship of the company with the consumer.”

The Data Privacy Act will require companies that collect personal data from more than 3,000 people a year to provide access to a concise privacy statement that is understandable to consumers and accurately describes their privacy policies.

This legislation allows consumers “to request, challenge accuracy and transfer or delete their data without compensation in the form of price or service discrimination on the part of businesses.”

The Data Privacy Act obliges companies that collect data on over 3,000 people a year “to prioritize the protection of consumer data by technological, administrative and physical means, depending on the risk of harm while ensuring that small businesses are protected from excessive demands and unnecessary regulations.”

This bill requires “companies that collect data from more than 3,000 people a year, with revenues of more than \$ 25 million a year, to appoint a Privacy Protection Officer to implement a culture of data protection and privacy in companies and to train the staff of the companies concerned.”

This legislation “extends the National Science Foundation's cybersecurity research to privacy strengthening technologies.”

The Data Privacy Act also gives the State Attorneys General and the Federal Trade Commission new authority to impose civil penalties for breaches.

This bill will be considered by the adequate US congressional committees.

3.1.1.2.7. Protecting Consumer Information Act of 2019:

Introduced to US Congress in 08/01/2019, by California Congressman Ted Lieu, this Act instructs the Federal Trade Commission “to review and possibly revise its customer information protection standards to ensure that they require certain consumer reporting agencies and service providers of this type to maintain adequate safeguards against cyber-attacks and related threats, to enable these standards for these agencies and providers, and for other purposes.”

This bill will be considered by the adequate US congressional committees.

3.1.1.2.8. Commercial Facial Recognition Privacy Act of 2019:

Introduced to US Congress in 08/01/2019, by sponsor Roy Blunt senior senator for Missouri, the Act restricts certain entities from “using facial recognition technology to identify or track an end-user without the end-user's affirmative consent, and for other purposes.”

This bill will be considered by the adequate US congressional committees.

3.1.2. Regulation examples at the state level:

In this subsection we will surf over laws and regulations concerning data privacy of the states of California, New York and Texas describing briefly the purposes of the regulations therein:

- California:

Data privacy regulations in the State of California affect apply to corporation and operators that collect and store data as well as their third party contractors. Operators and third party contractors are required to notify the affected data subject in case of any data breach informing him on what has happened, the nature of the information subject of the breach and the measures undertaken by the operator or his third party contractor to fix it.

Dissemination methods include both shredding and erasure.

California's regulations concerning data protection and privacy are considered to be pioneers in the sector and of high degree of seriousness, the regulations applies to social networking services, consumer information, privacy protection for children...

The regulations require non-financial companies to disclose to their consumers the nature of third parties which they are sharing the data with and the Consumer Confidentiality Rules requires disclosure of the nature of the collected and stored information about them with an option to "opt-out".

With regards to children online privacy the regulations:

- Limit the scope of online advertisements attracting children.
- Allow children to erase their data.

- New York:

The State of New York has enacted legislations that require operators and third party contractors to notify users of any breach affecting their data privacy, more importantly, the State legislatures are in course of enacting the "Stop Hacks and Improve Electronic Data Security Act" (or "SHIELD Act") with the aim of protecting sensitive personal /-information of the residents of New York

The SHIELD Act is a preventive measure to block data breaches before they happen since they have increased between 2015 and 2016 by 60% in the State.

The SHIELD Act applies to any business or entity that has New York residents as customers even if the entity is based outside New York with the exception of banks and financial companies which are regulated by the Financial Services Department with a different set of data privacy laws.

- Texas:

Texas is considered one of the proactive state in the US at this stage when it comes to regulating data privacy laws enacting many cybersecurity and privacy laws and taking identity theft very seriously.

Important data protection laws include the Student Data Privacy Act and the Cybersecurity Educational Act which don't only prevent data privacy infringement but focuses on encouraging the younger generation to adopt smart and healthy online practices at an early age even obliging public schools to offer coding classes.

The Acts require to provide users with breach notifications and violation of the laws is very costly: "\$100 per day per user not exceeding \$250,000 in total.

3.2. The European Union model: General Data Protection Regulation (GDPR):

3.2.1. Introduction:

The General Data Protection Regulation (EU) 2016/679 ("GDPR") is "an EU regulation aimed for data privacy protection of all individuals within the European Union (EU) and the European Economic Area (EEA) as well as the export of data outside the EU and EEA."

The GDPR's purpose is to enable individuals to have a say when it comes to controlling their online personal information while preserving a healthy environment for EU and non-EU business companies to operate and that is by unifying the regulation of data privacy between EU members.

Previous legislation on data protection within the EU is Directive 95/46/EC.

Provisions and requirements are set out by the GDPR affecting the processing of personal information of individuals in the European Economic Area (EEA) by legal entities whether they are located in the EEA or outside the EEA but engaging in the processing of personal information related to individuals who are residents of the EEA.

The regulation's full title is "Regulation 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 (Data Protection Directive)", it was enacted by the "European Parliament" and ratified by "the Council of the European Union" in 14/04/2016, with the implementation date being 25/05/2018.

The GDPR provides for the assignment of "Personal Data Controllers".

The mission of the personal data controllers is to implement adequate safeguards – technical or organizational – for data protection. Data processing software must be established based on those safeguards, developing techniques such as “pseudo-anonymization” or even “full anonymization”.

Processing software should establish default privacy settings that are maximized as much as possible without interference with the operational platform of the application.

Applying those safeguards should take into consideration that no information should be deemed public without the informed consent of the user and that no data shared online is sufficient by itself to identify a certain user.

According to the GDPR, personal data cannot be processed without a legal reason recognized by the legislation or if the data protection controller acquired a clear informed consent from a user which he is able to revoke any time and upon demand.

Entities processing personal information are required to unveil any data collection as well as provide a legal basis provided in the GDPR for that collection, furthermore, data processors are required to disclose the data storage time limit as well as the sharing of that data with third parties inside or outside the EEA.

The GDPR requires processors to provide users upon demand with “a copy of their collected and processed data in a portable format”, furthermore, the GDPR allows user to request their data to be erased under specified situations.

The GDPR provides for the assignment of “Data Protection Officers” or (DPOs), in all public governmental bodies which the main function deals with processing of personal information.

The mission of the DPO is to make sure that governmental bodies are compliant with the provisions and requirements of the GDPR.

The GDPR provides that: “Companies must report any data breach within 72 hours if this has a negative effect on the privacy of users”.

According to the GDPR, entities breaching the legislation “may be fined up to 20 million euros or up to 4% of the previous year's global annual turnover in the case of a business, according to the highest amount”.

The GDPR includes 99 articles as well as 173 recitals with explanatory remarks.

3.2.2. Scope:

The application of this regulation extends to the following:

- Entities collecting data from EU residents or “data controllers” are based in the EU.
- Entities processing and managing the data on behalf of data controllers are based in the EU.
- The data subject is an EU resident.
- Entities collecting and/or processing data outside the EU but deals with personal data of individuals who are residents of the EU. (in specific situations mentioned in the legislation).

According to the European Commission, "personal data are all information relating to an individual, whether relating to his private, professional or public life, which may be a name, personal address, photo, e-mail address, bank details, publications on social networking sites, medical information or the IP address of a computer”.

Article 4 of the GDPR provides definitions for “personal data”, “collector”, “processor”, “processing”, and “data subject”.

Recital 18 provides that “The regulation does not apply to the processing of data by a person for purely personal or domestic activity and therefore unrelated to a professional or commercial activity.”

Article 48 provides that “any judgment of a court or any administrative authority of a third country requiring a controller or a processor to transfer or disclose personal data cannot be recognized or enforced in any way without an international agreement, such as a mutual legal assistance treaty in force between the requesting third country (non-EU Member State) and the EU or a member State.”

This article protects against third country entities processing or collecting data on EU residents, from complying with a judicial order or security related requests from governmental bodies of these countries resulting in the handing over of personal information related to EU residents.

Articles 46 to 55 provide that “each Member State will set up an independent supervisory authority to hear and examine complaints and sanction administrative offenses, supervisory authorities in each Member State will cooperate with others, providing mutual assistance and organizing joint operations, if a company has several establishments in the EU, it will have a single supervisory authority as the main authority, depending on the location of its main establishment where the main processing activities take place, the lead authority will act as a one-stop-shop to oversee all processing activities for this company across the EU.”

The GDPR provides for the establishment of a “European Data Protection Board” or “EDPB” that will serve as a coordination tool for all the supervisory authorities across the EU.

3.2.3. Legal basis for “processing”:

The GDPR provides that the processing of data is allowed if an informed consent is provided by the user or if there is legal basis for processing. Article 6 provides these legal basis as follow:

- “The data subject has given consent to the processing of his personal data”;
- “Fulfill contractual obligations with a data subject or perform tasks at the request of a data subject in the process of concluding a contract”;
- “Comply with the legal obligations of the controller”;
- “Protect the vital interests of a data subject or other person”;
- “Perform a task in the public interest or on behalf of official authorities”;

- “For the legitimate interests of a controller or a third party, except where those interests are connected with the interests of the data subject or his rights under the Charter of Fundamental Rights” (particularly with children).

Article 7 provides that “If informed consent is used as the legal basis for processing, the consent must have been explicit for the data collected and each purpose used.”

Recital 32 also provides - on the informed consent by users – that “Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.”

Article 7 (3) provides that “Data subjects should be allowed to withdraw their consent at any time, and the process should not be more complicated than expected.”

Article 7 (4) provides that “A controller cannot refuse a service to users who refuse giving consent to processing data that is not strictly necessary to use the service.”

Article 8 (1) provides that “The Consent of children, defined in the regulation as being under 16 years of age must be given by a parent or a guardian of the child and be verifiable” It is left to the jurisdiction of each Member State of the EU to reduce it to 13 years of age.

Recital 171 provides that “If consent to processing has already been provided under the Data Protection Directive, a data controller must not recover it if the processing is documented and obtained in accordance with the requirements of the GDPR.”

3.2.4. Accountability:

In compliance with the GDPR, the data controller must put in action safeguards according to data protection principles by design and by default,

Article 25 provides that “Data protection by design and by default requires data protection measures to be incorporated into the development of business processes for products and services.”

These data protection measures undertaken by the data controller include pseudonymization of the data as soon as possible.

Recital 74 provides that “It is the responsibility of the data controller to implement effective measures and to be able to demonstrate compliance of the processing activities, even if the processing is carried out by a data processor on behalf of the controller.”

According to the GDPR and upon collection of the data, data subjects must be aware of the following rights:

- “The right to have access to information on the scale of the data collected.”
- “The right to have access to information on the legal basis for processing provided by the GDPR.”
- “The right to have access to information on the data storage period.”
- “The right to have access to information if the data is being shared with third parties inside or outside the EU.”
- “The right to have access to information on any automated decision making process based entirely on algorithms.”
- “The right to have access to information on their privacy rights according to the provisions of the GDPR.”

These privacy rights include:

- “The right to access their collected personal information.”
- “The right to have a view on how their data is being processed.”
- “The right to obtain a portable copy of the stored data.”
- “The right to retrieve their consent on the processing of their data anytime and upon demand.”
- “The right to erase their data in specified situations.”
- “The right to file a complaint before a data protection authority.”

Therefore, the user must always have the contact information of the data controller as well as the assigned data protection officer.

Article 35 provides that “Data protection impact assessments must be carried out when specific risks weigh on the rights and freedoms of data subjects. Risk assessment and

mitigation is required and prior approval by data protection authorities is required for high risks.”

3.2.5. Data Breaches:

Article 33 of the GDPR provides that “the data controller is legally obliged to inform the supervisory authority without undue delay, unless the breach wouldn’t jeopardize the rights and freedoms of individuals no more than 72 hours after the discovery of the data breach is required for the report to be made, the data processor will have to notify the controller without undue delay after learning of a personal data breach.”

Article 34 provides that “People must be notified if a negative impact is determined, notification to data subjects is not necessary if the controller has put in place appropriate technical and organizational safeguards that make the personal data unintelligible to any unauthorized person, such as encryption.”

3.2.6. Penalties:

Penalties for violations of data protection are provided in the criminal code of each Member State of the EU and the provisions of the GDPR.

Article 83 of the GDPR provides for the following penalties:

- “A written warning in cases of first non-intentional and non-compliance regular periodic data.”
- “A fine of up to EUR 10 million, or up to 2% of the previous year's global annual turnover whichever is greater in the event of a breach of the obligations of the controller and the processor, obligations of certification, and the obligations related to the supervisory body.”
- “A fine of up to EUR 20 million or 4% of the previous year's global annual turnover whichever is greater in case of infringement of the provisions related to the basic principles of processing, including the conditions of consent, the rights of the data subject, the transfer of data relating to a recipient located in a third country or an international organization, obligations arising from the law of the Member States, adopted in accordance with Chapter IX, the non-compliance with

an order or a temporary or permanent limitation to the processing or suspension of data flows by the supervisory authority, or lack of access.”

3.2.7. Exemptions:

The Regulation does not apply to the following cases:

- Matters of national security and ordinances by public authorities.
- Data collected within the frame of a statistical study or of a research.
- Data collected of a deceased user is under national law jurisdiction of each Member State.
- Employer-employee relationship (there is a special law that governs that).
- “Processing of personal data by a natural person in the context of a purely personal or domestic activity.”

For the GDPR to apply, it is crucial that the entity collecting or processing the data is engaging in an “economic activity” provided in the GDPR.

The GDPR affects entities having an “economic activity” defined in the legislation.

3.2.8. Impacts of the GDPR:

According to the GDPR, data controllers and processors were given a two years deadline to comply with the provisions and requirements of the GDPR, however, most of them have implemented the provisions before the deadline and not only for activities within the EU and the EEA but also worldwide.

Data collectors and processors notified their clients of the changes via e-mail and other notifications which resulted in a huge scale of online traffic.

The GDPR gives companies and websites two years to prepare their platforms to abide by the regulation but companies have already adapted their privacy policies and functions directly before the implementation not only in EU and EEA areas but worldwide.

Some of the notification e-mail have wrongfully provided that a new consent for processing data is required on the date of implementation of the GDPR, knowing that

according to the GDPR, a previous consent meeting the requirements of the legislation is valid.

The provisions of the GDPR were internationally adopted by legislative bodies, governments and private corporations which demonstrates the seriousness of the European legislation as a global reference for data protection and privacy.

Data collectors and processors and due to Article 33 that provides for breaches extensively, were encouraged to invest in acquiring new technologies that mitigate the vulnerabilities of the system even before they happen.

Some international online services have deprived EU-users access to their platforms or at least restricted their access to a reduced versions of their platforms with no advertisements and with less features compared to the original version of the service in order to mitigate the responsibilities resulting from the implementation of the GDPR.

3.3. The United Arab Emirates (UAE):

There is no federal law concerning data protection at the federal level that we are aware of, nevertheless data protection and privacy are regulated on the state level with legislations governing “the confidentiality and security of data”, furthermore, three free economic areas: Dubai International Financial Center, Abu Dhabi World Market and Dubai City Health Care, have related data protection regulations.

The most applicable regulation across the UAE related to data privacy is article 379 of the UAE criminal code that states “a person who, because of his profession, his art, or his status, is entrusted with a secret, is prohibited to use or disclose this secret without the consent of the person to which it belongs or otherwise in accordance with the law. “

The result of violating article 379 of the UAE criminal code is imprisonment for at least one year and/or a fine of 20,000 dirhams at least.

In article 379, terms like “secret”, “use”, or “disclose” are not defined but in practice, they include the concepts of “personal information”, “processing” and “transfer” in that order.

According to the article, the processing of personal information is allowed after acquiring the consent of the data subject, therefore it is important to have this consent before any use of personal information, thus preventing any breaches of the law.

The consent of the data subject may be acquired by signature or checking a box on a consent form, electronic signature...

According to the Regulatory Framework for Stored Securities and Electronic Payment Systems released by the central bank of the UAE, "Payment Service Providers" are required to retain identifying personal information and all related transactions.

"Payment Service Providers" are not allowed to process or share the retained data unless with the data subject, the central bank, a UAE court order, or as required by "Anti-Money Laundering and Anti-Terrorist Financing laws."

"Payment service providers" are required to retain data on any transaction and related users for 5 years, the retention process should happen within UAE borders excluding free economic zones.

The government of the Emirate of Dubai issued "the Dubai Law No. 26 of 2015" in an attempt to regulate dissemination and sharing of the data.

This law might be the only one in the world allowing governmental bodies the ability to oblige a private entity to disclose information related to a city in order to become open information.

Furthermore, we detected federal laws and other regulation affecting the subject of data privacy and protection as follows:

- "Constitution of the United Arab Emirates (Federal Law 1 of 1971)."
- "Criminal Code (Federal Law 3 of 1987 as amended)."
- "Law on Cybercrime (Federal Law 5 of 2012 on combating IT crime) (amended by Federal Law No. 12 of 2016 and Federal Decree No. 2 of 2018)."
- "Telecommunications Regulation (Federal Law by Decree No. 3 of 2003 as amended)."

3.4. *Lebanon:*

The “law on electronic transactions and personal data”, was promulgated in September 2018, by the Lebanese Parliament.

The law clearly sets out rules for the protection of personal data but the implemented legal framework is outdated (it was originally introduced in 2004) and not very well structured.

Matters related to the protection of personal data are embedded in chapter five of the law which contains five sections entitled “General provisions concerning the protection of personal data, the collection and processing of personal information, the actions necessary for the implementation of processing, the right of access and correction and the penal provisions.”

The law does not provide adequate safeguards relevant to the current reality of online data, thus, the provisions of this law are insufficient to protect the data of Lebanese residents.

Article 87 of the law, on “the general right to collect data”, is insufficient on determining legal basis justifications for data collection.

Article 94 discusses cases and situations where the obligation of acquiring a license for data processing does not apply.

The Law does not define terms such as “consent” nor the application of rules governing the conduct of data collectors.

Furthermore, the Law gives most authority to monitor the compliance of data collectors as well as the authority to licensing and all decision making aspects related to the legislation, solely to the Minister of Economy and Trade without any supervision or control by the legislative or judicial branches.

According to article 95, the minister has the right to approve or deny access to data by third parties and the transfer of the data outside Lebanon.

In addition, the law is not yet applicable since the Ministry of Economy and Trade did not establish the adequate infrastructure such as competent human resources, a website facilitating the licensing of data processing...

The provisions of article 97 are not sufficient to protect against abuse of power, since it allows the Ministries of interior and defense to issue licenses pertaining to the collection of data on "internal or external security of the state" without mentioning any mechanism to monitor such licensing. Furthermore, the law doesn't define the term "internal or external security of the state".

In Lebanon data privacy is regulated by the following provisions and laws:

- "Articles of Law 140/1999."
- "Law of 3 September 1956 on Banking Secrecy."
- "Articles 579, 580 and 581 of the Penal Code relating to the breach of secrets."
- "Article 7 of the Code of Medical Ethics."
- "Articles 51 and 58 of the Consumer Protection Code."
- "Law on electronic transactions and personal data."

Conclusion

In the first chapter of this dissertation, we have introduced the concept of “Social Data Analytics” stating that it originated from “Big Data” from which “Social Data” can be extracted in order to be analyzed, we have also described the social data revelation, in particular, the rise of web 2.0 and social networking services. We also mentioned the types of data generated, how it is obtained and the process to do so. Furthermore, we described the relation between social data and the business sector as well as the computation of social sciences and business intelligence made possible by social data analytics.

In the second chapter, we have discussed “privacy concerns” and their related platforms starting by the causes of online privacy concerns, then its relation with data access methods. We have also mentioned the benefits acquired from “social data analytics” and the potential dangers including identity theft, preteens and early teenagers, sexual predators, stalking and other potential dangers, we have also discussed the most notorious social networking platforms such as Facebook and Twitter among others and the disadvantages of their privacy policies. Furthermore, we have discussed the Facebook and Cambridge Analytica incident and the resulting Testimony of Mark Zuckerberg, Facebook CEO, to the US Congress.

In the third and final chapters, we have identified, described and interpreted different jurisdictions regulating data privacy, including the United States of America both on the federal and the state level, the European Union, the United Arab Emirates, and Lebanon.

No matter the degree of complexity of data protection and privacy safeguards embedded in a software, a breach is always a possibility by third parties whether by government agencies or malicious individuals with the adequate knowledge, thus full security becomes impossible.

Thus, if the question is whether we can reach total individual privacy online then the answer is no, unless the individual refrains completely from sharing data or personal information throughout all social networking services.

Therefore, regulations should focus on combatting the uninformed consent of online users into sharing “personal identifiable information” on social networking services while preserving a healthy business environment as well as enhancing the opportunities offered by social data analytics to researchers.

The legal framework must set out clear and thoroughly defined provisions for businesses to adhere with and for the public to understand, it should also present incentives encouraging data collectors and processors to invest in data protection technology.

Businesses need clearer rules and individuals need to be able to encourage businesses to secure their data.

The legal framework for data protection and privacy should be limited to a single legislation for better reference and understanding.

The legal framework should apply to all sectors of the economy not only tech-companies, it should incorporate data protection and privacy as a segment of corporate social responsibility (CSR), as an organizational structural risk and a compliance requirement for all institutions.

The legal framework must encourage companies to adopt preventive measures with regards to data protection and privacy, rather than fixing the breach after the fact with the legal procedure that comes with it.

Organizations must provide data subjects with an easy access to their collected and stored information, the ability to delete or alter upon demand and at any time this information therefore adopting the “right to be forgotten”, it should also require companies to provide data supervisory authorities with a timely risk assessment report.

The legal framework should establish a single data protection authority making sure of the compliance with rules and regulations as well as assigning “data protection officer” to each entity with the mission of making sure that corporations are adhering to the legislation.

The legal framework should acknowledge the consequences of data breaches as well as setting clear procedure to neutralize the threats.

References

A formal definition of Big Data based on its essential features. (n.d.). Retrieved from <http://www.emeraldinsight.com/doi/abs/10.1108/LR-06-2015-0061>.

Andreas, K. and Haenlein, M. (2018). Siri, Siri in my Hand, who's the Fairest in the Land? [Online] www.sciencedirect.com. Available at: <https://www.sciencedirect.com/science/article/pii/S0007681318301393>.

American Civil Liberties Union. (December 16, 2010). Commerce department releases important report urging comprehensive privacy protections. Retrieved from <https://www.aclu.org/technology-and-liberty/commerce-department-releases-important-report-urging-comprehensive-privacy-pr>

American Civil Liberties Union. (n.d.). Retrieved from <https://www.aclu.org/technology-and-liberty/government-requests-twitter-users-personal-information-raise-serious-constitution>

Alex Heath, Business Insider. (2015, October 30). Why you don't need to freak out about Snapchat's new privacy policy. Retrieved from <http://www.businessinsider.com/snapchat-privacy-policy-update-explained-2015-10>

Analysis by Chris Cillizza, CNN Editor-at-large. (2018, April 11). How the Senate's tech illiteracy saved Mark Zuckerberg. Retrieved from <https://edition.cnn.com/2018/04/10/politics/mark-zuckerberg-senate-hearing-tech-illiteracy-analysis/index.html>

ACLU v. Mukasey -- Challenge to Internet Censorship. (n.d.). Retrieved from http://www.epic.org/free_speech/copa/

Afifi-Sabet, Keumars (3 May 2018). "Scammers are using GDPR email alerts to conduct phishing attacks" . IT PRO.

Big Data for Development: From Information- to Knowledge Societies. (n.d.). Retrieved from <https://ssrn.com/abstract=2205145>.

Bennet, J. n.d. Internet Memes. [online]. Available at: "Archived copy" (<https://web.archive.org/web/20110720113942/> and <http://2010.newsweek.com/top-10/internet-memes/the-star-wars-kid.html>). Archived from the original (<http://2010.newsweek.com/top-10/internet-memes/the-star-wars-kid.html>).

Bowers, T. 2008. Employers who check out job candidates on MySpace could be legally liable. [Online]. Available at: <http://www.techrepublic.com/blog/career/employers-who-check-out-job-candidates-on-myspace-could-be-legallyliable/338>

BBC News. 2008. Crew sacked over Facebook posts. Available at: <http://news.bbc.co.uk/1/hi/uk/7703129.stm>

Bianca Bosker, Virtual Guide To Facebook's Privacy Changes Over Time, 2010.

Retrieved from http://www.huffingtonpost.com/2010/05/07/facebook-privacy-changes_n_568345.html

Burnham, Kristin. "5 Ways Snapchat Violated Your Privacy, Security -

InformationWeek." InformationWeek. 5

(<http://www.informationweek.com/software/social/5-ways-snapchatviolated-your-privacy-security/d/d-id/1251175>).

Burgess, M. (2017, January 27). New presidential order could wreck US-EU Privacy Shield. Retrieved from <https://www.wired.co.uk/article/trump-privacy-shield-data>

. Burgess, Matt. "Help, my lightbulbs are dead! How GDPR became bigger than Beyoncé" . Wired.co.uk.

Bălăiți, George (9 November 2018). "English Translation of the Letter from the Romanian Data Protection Authority to RISE Project" . Organized Crime and Corruption Reporting Project. Archived from the original on 9 November 2018.

Cave, A. (2018, November 4). What Will We Do When The World's Data Hits 163 Zettabytes In 2025? Retrieved from <https://www.forbes.com/sites/andrewcave/2017/04/13/what-will-we-do-when-the-worlds-data-hits-163-zettabytes-in-2025/#4df450a1349a>.

Cortez Masto Introduces DATA Privacy Act. (2019, February 28). Retrieved from <https://www.cortezmasto.senate.gov/news/press-releases/cortez-masto-introduces-data-privacy-act>

Commercial Facial Recognition Privacy Act of 2019 (S. 847). (n.d.). Retrieved from <https://www.govtrack.us/congress/bills/116/s847>

Chen, Brian X. (23 May 2018). "Getting a Flood of G.D.P.R.-Related Privacy Policy Updates? Read Them" . The New York Times. ISSN 0362-4331 .

Data, data everywhere. (2010). Retrieved from <http://www.economist.com/node/15557443>.

Dwyer, C., Hiltz, S., & Passerini, K. "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace" (<http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1849&context=amcis2007>). Association for Information Systems AIS Electronic Library (AISeL). AMCIS 2007 Proceedings.

Damon, Cody (9 March 2011). "Do Facebook Friends Influence Advertising?" (<http://socialmediatoday.com/codydamon/276901/do-facebook-friends-influence-advertising>).

Electronic Privacy Information Center, Initials. (2011, January 18). Facebook drops plan to disclose users' home addresses and personal phone number. Retrieved from <http://epic.org/privacy/socialnet/>

EUR-Lex — Access to European Union law — choose your language. (n.d.). Retrieved from <http://Eur-lex.europa.eu>

"EU gov't and public health sites are lousy with adtech, study finds" . TechCrunch.

"EU citizens being tracked on sensitive government websites" . Financial Times.

Facebook users worldwide 2018. (n.d.). Retrieved from

<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>

Facebook-Online Social Interaction/Privacy. (n.d.). Retrieved from

<https://sites.google.com/site/cat200group5/home/invasive-privacy-agreements/2>

Fitzpatrick, A. (2012, May 4). Study Says Facebook Privacy Concerns Are on the Rise - Is It Accurate? Retrieved from <http://mashable.com/2012/05/04/facebook-privacy-concerns-study/>

Facebook can tell when teens feel insecure. (2017, May 1). Retrieved from

<https://www.usatoday.com/story/tech/news/2017/05/01/facebook-can-tell-when-teens-feel-insecure-advertiser-target/101158752/>

Facebook to send Cambridge Analytica data-use notices to 87 million users today.

(2018, April 9). Retrieved from <https://www.nbcnews.com/tech/social-media/facebook-send-cambridge-analytica-data-use-notices-monday-n863811>

Facebook says 300,000 Australians may have had their data 'improperly shared'. (2018, April 5). Retrieved from <http://www.abc.net.au/news/201804-05/facebook-raises-cambridge-analytica-estimates/9620652>

Facebook Cambridge Analytica Scandal Aftermath. (n.d.). Retrieved from
<https://privacyhub.net/facebook-cambridge-analytica-scandal-aftermath/>

"Fall asleep in seconds by listening to a soothing voice read the EU's new GDPR legislation" . The Verge.

Good night, Posterous. (n.d.). Retrieved from
<http://swathidharshananaidu.posterous.com/social-data-revolution.>

Ganis, Matthew; Kohirkar, Avinash (2015). Social media Analytics: Techniques and insights for Extracting Business Value Out of Social Media. New York: IBM Press. pp. 40–137.

Ganis, Matthew; Kohirkar, Avinash (2015). Social media Analytics: Techniques and insights for Extracting Business Value Out of Social Media. New York: IBM Press. pp. 40–137.

Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networking Sites (The Facebook Case).

Grenoble, Ryan (2012-10-26). "Bogomil Shopov, Bulgarian Tech Consultant: 1 Million Users' Private Facebook Data Available Online For \$5 (VIDEO)"
(http://www.huffingtonpost.com/2012/10/26/bogomil-shopov-facebook-data_n_2024133.html). The Huffington Post.

Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networking Sites (The Facebook Case). [Online]. p. 8. Available at:
<http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf>

"GDPR mayhem: Programmatic ad buying plummets in Europe" . Digiday. 25 May 2018.

"GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook" (PDF).

Hilbert, M., & López, P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. Retrieved from
<https://www.martinhilbert.net/worldinfocapacity-html/>.

Havenstein, H. 2008. One in five employers uses social networks in the hiring process. [Online]. Available at:

http://www.computerworld.com/s/article/9114560/One_in_five_employers_uses_social_networks_in_hiring_process

Henson, Bill; Reynes W. Reyns; Bonnie S. Fisher (3 March 2011). "Security in the 21st century: examining the link between online social network activity, privacy, and interpersonal victimization". *Criminal Justice Review*. 36 (253): 253–268.
doi:10.1177/0734016811399421
(<https://doi.org/10.1177%2F0734016811399421>).

Harvard Business Publishing. (n.d.). Retrieved from
http://cb.hbsp.harvard.edu/cb/web/he/product_view.seam?R=808128-PDFENG&T=EDC&C=PURCHASED_MATERIALS&CD=16117304&CS=90ae2ef93335be224703aca3962ad383

Harvard Business Publishing. (n.d.). Retrieved from
http://cb.hbsp.harvard.edu/cb/web/he/product_view.seam?R=808128-PDFENG&T=EDC&C=PURCHASED_MATERIALS&CD=16117304&CS=90ae2ef93335be224703aca3962ad383

Horwitz, J. (2018, April 5). Outside the US, the Philippines saw the most Facebook user data go to Cambridge Analytica. Retrieved from
<https://qz.com/1245355/outside-us-philippines-saw-most-facebook-user-data-go-to-cambridge-analytica/>

Hern, Alex (21 May 2018). "Most GDPR emails unnecessary and some illegal, say experts" . The Guardian.

"How Europe's GDPR Regulations Became a Meme" . Wired.

"Here Are Some of the Worst Attempts At Complying with GDPR" . Motherboard. 25 May 2018.

Heisei 28 (Kyo) 45 (S. Ct., Jan. 31, 2017), http://www.courts.go.jp/app/hanrei_jp/detail2?id=86482 (click Chinese

characters beside the PDF icon), archived at <https://perma.cc/4RL2-JXMM> & <https://perma.cc/UU8T-AP2K>.

Internet Privacy Laws in America: A Guide to All 50 States. (2019, February 26). Retrieved from <https://termly.io/resources/articles/data-privacy-laws-by-state-a-complete-guide/#data-privacy-laws-by-state>

Journal, R. (n.d.). That 'Internet of Things' Thing. Retrieved from <http://www.rfidjournal.com/articles/view?4986>.

Judge tells DoJ "No" on search queries. (2006, March 17). Retrieved from <http://googleblog.blogspot.com/2006/03/judge-tells-doj-no-on-search-queries.html>

Kitchin, R., & McArdle, G. (2016). What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets. Retrieved from <https://journals.sagepub.com/doi/abs/10.1177/2053951716631130>.

Kovacs, G. (n.d.). Tracking our online trackers. Retrieved from https://www.ted.com/talks/gary_kovacs_tracking_the_trackers?language=en

Kozlowska, Hanna (April 4, 2018). "The Cambridge Analytica scandal affected 87 million people, Facebook says" (<https://qz.com/1245049/the-cambridge-analytica-scandal-affected-87-million-people-facebook-says/>). Quartz.

Liu, Libo, Cheung, Christy M.K., and Lee, Matthew K.O. 2016. "An empirical investigation of information sharing behavior on social commerce sites." *International Journal of Information Management* 36(5): 686-699.

Lori Andrews (10 January 2012). *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* (<https://books.google.com/books?id=XCtKe6Mjx-0C>). Simon and Schuster. ISBN 978-1-4516-5051-8.

Lanxon, Nate (25 May 2018). "Blocking 500 Million Users Is Easier Than Complying With Europe's New Rules" . Bloomberg.

Law. (n.d.). Retrieved from <https://www.dlapiperdataprotection.com/index.html?t=law&c=ZA>

Law. (n.d.). Retrieved from <https://www.dlapiperdataprotection.com/index.html?t=law&c=AE>

Law. (n.d.). Retrieved from <https://www.dlapiperdataprotection.com/index.html?t=law&c=BR>

Manyika, James; Chui, Michael; Bughin, Jaques; Brown, Brad; Dobbs, Richard; Roxburgh, Charles; Byers, Angela Hung (May 2011). "Big Data: The next frontier for innovation, competition, and productivity" (http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation). McKinsey Global Institute.

Mills, Max. "Sharing Privately: The Effect Publication on Social Media Has on Expectation of Privacy" EBSCOhost. Journal of Media Law.

Masnack, Mike (19 November 2018). "Yet Another GDPR Disaster: Journalists Ordered To Hand Over Secret Sources Under 'Data Protection' Law"

'Not all my friends need to know? : A qualitative study of teenage patients, privacy, and social media. (2013, January 1). Retrieved from <https://academic.oup.com/jamia/article/20/1/16/2909199/Not%2Dall%2Dmy%2Dfriends%2Dneed%2Dto%2Dknow%2Da%2Dqualitative>

'Not all my friends need to know? : A qualitative study of teenage patients, privacy, and social media. (2013, January 1). Retrieved from <https://academic.oup.com/jamia/article/20/1/16/2909199/Not-all-my-friends-need-to-know-a-qualitative>

Nixon, Ron (2017-09-28). "U.S. to Collect Social Media Data on All Immigrants Entering Country"(<https://www.nytimes.com/2017/09/28/us/politics/immigrants-social-media-trump.html>). The New York Times. ISSN 0362-4331 (<https://www.worldcat.org/issn/0362-4331>)

Nieva, Richard (June 13, 2018). "Most Facebook users hit by Cambridge Analytica scandal are Californians" ([https:// www.cnet.com/news/most-facebook-users-hit-by-cambridge-analytica-scandal-are-californians/](https://www.cnet.com/news/most-facebook-users-hit-by-cambridge-analytica-scandal-are-californians/))

Paul, Ian. "Snapchat Clarifies Privacy Policies after Terms of Service Change Freaks out Users." PCWorld. 2 November 2015. Web. 28 February 2016.

Peter Chapman, Sex Offender, Admits Rape And Murder Of Teen He Ensnared On Facebook. (2017, December 6). Retrieved from http://www.huffingtonpost.com/2010/03/08/peter-chapman-admits-usin_n_489674.html

Profiting With Facebook Ads: Affiliate Confession. (2008, August 13). Retrieved from <http://www.affiliateconfession.com/2008/08/13/profitting-with-facebook-ads/>

Privacy alert over 'scary' site which publishes home addresses of Twitter users from around the world. (2012, August 24). Retrieved from <http://www.dailymail.co.uk/sciencetech/article-2192554/Privacy-concerns-scary-site-publishes-twitter-users-home-addresses.html>

Privacy Act of 1974. (n.d.). Retrieved from <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279>

Privacy Act of 1974. (2015, July 17). Retrieved from <http://www.justice.gov/opcl/privstat.htm>

Password Protection Act of 2012 (2012 - H.R. 5684). (n.d.). Retrieved from <https://www.govtrack.us/congress/bills/112/hr5684>

Protecting Consumer Information Act of 2019 (H.R. 331). (n.d.). Retrieved from <https://www.govtrack.us/congress/bills/116/hr331>

"Privacy notices under the EU General Data Protection Regulation". Ico.org.uk. 19 January 2018.

Quinn, Kelly. "Why We Share: A Uses and Gratifications Approach to Privacy Regulation in Social Media Use". EBSCOhost. Journal of Broadcasting & Electronic Media.

Reid Hoffman (June 26, 2009). "Future of Jobs & Social Data Revolution" (<http://www.techaffair.com/2009/06/reid-hoffman-ceo-of-linkedin-on-the-future-of-jobs-social-data-revolution/>). Techaffair.com.

Roythornes Solicitors. 2011. The employment law dangers of Social Networking. [Online]. Available at: <http://www.opportunitypeterborough.co.uk/bondholder/events/the-employment-law-dangers-of-social-networking> .

Richard Lardner. (March 16, 2010). Your new Facebook 'friend' may be the FBI. Retrieved from http://www.msnbc.msn.com/id/35890739/ns/technology_and_science-security/

Rosenberg, Matthew; Confessore, Nicholas; Cadwalladr, Carole (March 17, 2018). "How Trump Consultants Exploited the Facebook Data of Millions" (<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trumpcampaign.html>)

"Ruling on Google subpoena"

(http://www.google.com/press/images/ruling_20060317.pdf)

Roberts, Jeff John (25 May 2018). "The GDPR Is in Effect: Should U.S. Companies Be Afraid?" .

Science, L. How Big Is the Internet, Really? Retrieved from

<https://www.livescience.com/54094-how-big-is-the-internet.html>

Social Networking Privacy: How to be Safe, Secure and Social. (n.d.). Retrieved from

<https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social#hindering-job-seekers>

"Social Media and Cyber Stalking Facts - Advice and Tips on Staying Protected"

(<http://www.seomworld.com/2013/09/social-media-and-cyber-stalking-facts.html#.U5U6LZRdWUw>).

Sky News. 2009. Sacked for Calling Job Boring on Facebook. [Online]. Available at:

<http://news.sky.com/skynews/Home/UK-News/Facebook-Sacking-Kimberley-Swann-From-Clacton-Essex-SackedFor-Calling-Job-Boring/Article/200902415230508>

Snapchat's new Snap Map feature raises privacy concerns. (2017, June 26). Retrieved

from <https://abcnews.go.com/Lifestyle/snapchats-snap-map-feature-raises-privacy-concerns/story?id=48271889>

Social Networking Online Protection Act (2012 - H.R. 5050). (n.d.). Retrieved from <https://www.govtrack.us/congress/bills/112/hr5050>

S. 189: Social Media Privacy Protection and Consumer Rights Act of 2019. (n.d.). Retrieved from <https://www.govtrack.us/congress/bills/116/s189/summary>

Social Media Use in Clearance Investigations Act of 2019 (H.R. 1065). (n.d.). Retrieved from <https://www.govtrack.us/congress/bills/116/hr1065>

State of Privacy Lebanon. (n.d.). Retrieved from <https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon#dataprotection>

Transport, D., Fox, C. and Publishing, S. (2019). Data Science for Transport - A Self-Study Guide with Computer Exercises | Charles Fox | Springer. [Online] Springer.com. Available at: <https://www.springer.com/us/book/9783319729527>.

Twitter: number of active users 2010-2018. (n.d.). Retrieved from <https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/>

The Three Elements of Successful Data Visualizations. (2013, April 19). Retrieved from <https://hbr.org/2013/04/the-three-elements-of-successf>.

Tracy Mitrano. (November–December 2006). A Wider World: Youth, Privacy, and Social Networking Technologies.

"Twitter Privacy Policy" Twitter, effective June 23, 2011, retrieved February 13, 2012.
www.twitter.com/privacy.

"The Internet Created a GDPR-Inspired Meme Using Privacy Policies" . Adweek.

"The Data Protection Officer (DPO): Everything You Need to Know" . Cranium and HackerOne. 20 March 2018.

UniCredit has stopped using Facebook for advertising: CEO. (2018, August 7).
Retrieved from <https://www.reuters.com/article/us-facebook-unicredit/unicredit-has-stopped-using-facebook-for-advertising-ceo-idUSKBN1KS1N5>

Vogel, Kenneth (7 July 2015). "Cruz partners with donor's 'psychographic' firm". Politico.

We Can't Give Up on Privacy! Webopedia TechBytes Blog. (n.d.). Retrieved from
<https://www.webopedia.com/Blog/we-cant-give-up-on-privacy.html>

Wayback Machine. (n.d.). Retrieved from
<https://web.archive.org/web/20180330152735/>

Wolfe, Daniel (October 21, 2009). "Bad Friends"
(<https://libproxy.berkeley.edu/login?qurl=http%3a%2f%2fsearch.ebscohost.com%2flogin.aspx%3fdirect%3dtrue%26db%3dbth%26AN%3d44791244>)

%26site%3ded-s-live). American Banker. 174 (192): 5 – via University of California Berkeley Library.

"Why Government Use of Social Media Monitoring Software Is a Direct Threat to Our Liberty and Privacy" (<https://www.aclu.org/blog/privacy-technology/surveillance-technologies/why-government-use-social-media-monitoring>).

"What information must be given to individuals whose data is collected?". Europa (web portal)

Wehlander, Caroline (2016). "Chapter 2 "Economic activity": criteria and relevance in the fields of EU internal market law, competition law and procurement law". In Wehlander, Caroline. Services of general economic interest as a constitutional concept of EU Law (PDF). The Hague, Netherlands: TMC Asser Press. pp. 35–65.

"What Percentage of Your Software Vulnerabilities Have GDPR Implications?" (PDF). HackerOne. 16 January 2018.

"What might bug bounty programs look like under the GDPR?" . The International Association of Privacy Professionals (IAPP). 27 March 2018.

Zetlin, M. (2018, April 12). Mark Zuckerberg Testified Before Congress. Here Are the Strangest and Funniest Questions They Asked. Retrieved from <https://www.inc.com/minda-zetlin/mark-zuckerberg-congress-hearings-funny-stupid-questions.html>