Summer 6-15-2022

Nudging Users Towards Data Privacy

Ossama Hanafy
The American University in Cairo AUC, ossama_hanafy@aucegypt.edu

The American University in Cairo

School of Global Affairs and Public Policy

Nudging Users Towards Data Privacy

A Thesis Submitted to the
Department of Law
in partial fulfillment of the requirements for
LLM degree in International and Comparative Law

By

Ossama Hanafy

Fall 2021

The American University in Cairo
School of Global Affairs and Public Policy

NUDGING USERS TOWARDS DATA PRIVACY

A Thesis Submitted by

Ossama Hanafy Hassan Hanafy

to the Department of Law

Fall 2021

in partial fulfillment of the requirements for the
LL.M. Degree in International and Comparative Law has been approved by

Hani Sayed (Supervisor)
Associate Professor ____________________
Law Department
The American University in Cairo

Thomas Skouteris (First Reader)
Associate Professor ____________________
Law Department
The American University in Cairo

Jason Beckett (Second Reader)
Assistant Professor ____________________
Law Department
The American University in Cairo

Graduate Program Director	**Date**	**School Dean**	**Date**
____________________	________	______________________	________
Thomas Skouteris		Ambassador Dean Fahmy	

DEDICATION

I dedicate this work to my father's soul, and mother who have been a source of enlightenment and inspiration throughout my entire life. To my caring, loving, and supportive wife: my deepest gratitude. This work could not have been accomplished without your support and encouragement.

The American University in Cairo

School of Global Affairs and Public Policy

Department of Law

NUDGING USERS TOWARDS DATA PRIVACY

Ossama Hanafy

Supervised by Professor Hani Sayed

ABSTRACT

The internet challenges users' privacy in unpreceded ways. Technology companies collect massive amounts of data from online users. They use algorithms that can track and analyze each activity by each user. Even though many users worry about their online privacy, they keep revealing more personal data. This study explores the causes behind online privacy erosion. While tech companies and governments aim to achieve economic and political goals, users are motivated by social motives. Online Privacy erosion leads to many harms to individuals and societies while collecting, processing, and disseminating data. Moreover, this study argues that the current legal approaches, especially the GDPR and the Egyptian law for data protection, fail to effectively protect data privacy because they could not overcome the complexity of data privacy. Online users act irrationally due to several influences that affect their decisions and undermine their ability to manage their privacy. Therefore, this study argues that applying the libertarian paternalism theory on online privacy would help to promote privacy. Nudging users towards online privacy can be done by architecting choices in a manner that alters users' behavior in a predictable way without omitting any options or changing their economic incentives. Nudges preserve online self-management because they do not forbid any options. They also overcome the privacy complexity by simplifying the options. Finally, this study introduces some nudges designs that can enhance users to protect their privacy.

KEY WORDS: Online Privacy – Data Protection - Libertarian Paternalism – Nudges — Online Self-management

TABLE OF CONTENTS

I. Introduction

The internet has changed our lives in significant ways. Billions of individuals use it on a daily basis for multiple purposes. They depend on the internet to buy different products and services, get information, conduct researches, and socialize with friends. Whether explicitly or implicitly, users disclose personal information in order to benefit from the services of different websites and apps. While using the internet, billions of data points were collected and transmitted. Tech companies make huge profits from those data. In 2022, the big data market is expected to worth 274 billion dollars.[1] Data is the raw material for this industry. Thus, when data become the most valuable resource on the planet, privacy would be the most violated right.

Before the emergence of the internet, privacy was confined to physical actions that are mostly related to one's body and home. Informational privacy was raised with the development of the press and media. However, the internet challenged the right to informational privacy in unpreceded ways. Social media platforms facilitated the disclosure of data. Users reveal many personal data without noticing the risks of their behavior. They also give permission to many companies to know their names, location, age, sex, images, family members, friends, contact list, and online habits. Moreover, algorithms have the ability to track, record, and analyze each activity of each user on the internet. They can reveal sensitive information by combining different pieces of data. Such practices have endangered the right to privacy.

The privacy violations are motivated by commercial, political, and social motivations. Tech companies depend on data to categorize the users in order to effectively market their ads. They gain billions of dollars from our data. In addition, analytics companies collect and analyze the personal data of millions of people in order to understand their political and social beliefs. Governments hire such companies to influence the people in order to achieve political objectives. On the other hand, people are the victims of their weaknesses. They reveal too much information to fulfill their social needs. Most users want to create an attractive profile in order to make new friends and profound their relationship with current ones. Social media platforms provide them with the capabilities to communicate with

[1] Revenue from big data and business analytics worldwide from 2015 to 2022, https://www.statista.com/statistics/551501/worldwide-big-data-business-analytics-revenue/.

family members and friends easily. They like to talk and share their experiences with others. They disclose a vast amount of data without paying attention to the practices' consequences.

However, defining the right to privacy is challenging. It is too vague and complex. It is embodied in various legal rules like trespassing, wiretapping, illegal search and seizure, defamation, blackmailing, extortion, identity theft, and fraud. As Professor Solove argues, "privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[2] In my opinion, informational privacy should be defined based on the privacy harms that affect individuals and society. Many privacy harms occur to individuals while collecting, processing, and disseminating the data. Data collection involves interrogation and surveillance, while data processing deals with data storage, usage, aggregation, and manipulation. Throughout those activities, many harms affect individuals. Meanwhile, data dissemination involves various kinds of harms like breach of confidentiality, defamation, blackmailing, and distortion. On the other hand, societies suffer from privacy violations. Due to the personalization technology, people live in echo chambers because algorithms show the user what reflects his/her believes and preferences. Such technologies prevent users from forming balanced opinions because algorithms would not show up other arguments, which leads to polarization and the spread of misbeliefs. In the meantime, tech companies and governments can exploit such technologies to influence the people, which threatens democracy.

The question that arises is to what extent can law intervene to protect individuals from their own mistakes? The rule is: governments should refrain from coercing individuals as long as their actions do not harm other individuals.[3] A Citizen is autonomous and has the freedom to choose in a self-interested manner; this self-management should be protected by the state, not the opposite. Hence, people have the right to abandon their privacy as long as they agree to do so and they do not harm others, as many scholars and tech companies

[2] Daniel J. Solove, Conceptualizing Privacy, 90 CALIF. L. REV. 1087 (2002), at 1088.

[3] See Joseph William Singer, The Legal Rights Debate in Analytical Jurisprudence from Bentham to Hohfeld, 6 Wis. L. Rev. 975-1060 (1982).

argue. However, behavioral economics scholars proved that people do not choose what is the best in their interest. Despite the harm, people smoke cigarettes, eat unhealthy foods, and abandon their privacy. Thaler and Sunstein propose the "Libertarian Paternalism" theory as a solution that can promote individuals' welfare without affecting their freedom of choice.[4] Based on scientific experiments, people act irrationally because they are influenced by different factors. Those influences are unavoidable; there is no neutrality in choice architecture. Therefore, they concluded that people's decisions should be improved by using nudges that can change their behavior in a predictable way without omitting any choices.

In this study, I argue that using libertarian paternalistic techniques can promote online privacy in a manner that can complement other legal tools. This study illustrates how data subjects act irrationally regarding their privacy. Even though there is an increasing concern regarding online privacy, people reveal recklessly many personal information. They are influenced by many influences. They have to disclose personal information to benefit from internet services and to communicate with their friends. Tech companies exploit this advantage to make people disclose more information. Meanwhile, online privacy choices are complex, which impede users' ability to make rational decisions.

On the other hand, this study critically analyzes the proposed legal solutions and shows their ineffectiveness in dealing with online privacy. While some scholars argue for the coercion of privacy, others argue for the non-intervention of the state. In my opinion, both fail to achieve the required balance in the data market. The first proposal would lead to the collapse of the data market because it will severely hinder the flow of data which internet service providers depend on to provide their services; it also demolishes individual autonomy. Meanwhile, the non-intervention advocates ignore the harms of privacy erosion and the market failure in regulating the data.

Moreover, the user's empowerment policy is ineffective in promoting online privacy. The general data protection regulation (GDPR) and the new Egyptian for personal data protection No. 151 of 2020 choose to empower citizens with a bundle of rights.[5] However,

[4] See Cass R. Sunstein & Richard H. Thaler, Behavioral Economics, Public Policy, and Paternalism: Libertarian Paternalism, 93 American Economic Rev. 175 (2003).

[5] General Data Protection Regulation, Regulation (EU) 2016/679 (27 April 2016); Law No. 151 of 2020 (Law of Personal Data Protection).

there are real concerns regarding the ability of users to use those rights. Online users are not aware of the potential risks. They also are under pressure to accept the services providers' terms in order to benefit from their services. In addition, small businesses have to spend a huge amount of money to implement new laws which threaten their growth. As a result, the proposed legal solutions are not effective in dealing with the online privacy issue, which leaves a gap that nudges can fill.

Chapter two of this study explains the data collection methods and the erosion of online privacy. It also aims to understand the problem by exploring the motives of tech companies, governments in collecting data, and the users' motives in disclosing their personal data. Chapter three aims to define informational privacy by identifying the privacy harms that occur to individuals and societies while collecting, processing, and disseminating the data. Chapter four deals with the self-management problem regarding online privacy. It evaluates the current legal approaches, and argues that the proposed legal solutions do not offer an effective solution for the beforehand issue. In addition, it demonstrates the libertarian paternalism arguments in proving individuals' irrationality and the inevitability of choices' influences while replying to the theory's critiques. Finally, chapter five applies the libertarian paternalism theory on the online privacy issue. It shows how data subjects act irrationally regarding their online behavior. Then, it details how using nudges can promote online privacy, and introduces some examples of nudges that can be implemented by online platforms to improve privacy.

II. Erosion of Online Privacy

A. How Does the Internet Challenge the Right to Privacy?

The internet has become essential in the life of millions of people. In 2021, the number of active internet users worldwide is 4.66 billion, up from 3.97 billion in 2019.[6] The emergence of social media platforms has led to a vast increase in the number of users. Facebook, for example, has over 2.2 billion monthly active users, which represent almost half of internet users worldwide.[7] Most users spend hours each day using different apps and accessing websites. Throughout that daily use, millions of users reveal different kinds of information about their lives, whether explicitly or implicitly. To use internet service providers (ISP) services, users grant them access to their contacts, location, images, and activities over their devices. They also post about their daily activities and share their thoughts on social media.

On the other side of the internet, tech companies receive and restore those billions of points of data. They use those data to understand the behavior of users and build a profile for each one. They develop complex algorithms that analyze users' likes, posts, search history, location, and other information to enhance their customers' experience. They determine search results and which articles, videos, websites, and advertisements would appear on their screens according to each one's preferences.[8] However, such practices are associated with intense privacy concerns.

The internet has declared a new age to the right to privacy. Before the internet era, privacy meant "the right to be let alone," which provides individuals with protection from physical intervention in one's private affairs. The private sphere is usually violated by a physical act. The violator needs to act in the real world to reveal what one hides. Actions like unlawful surveillance, unwarranted search and seizure, and intrusion are done by intervening physically in one's private sphere. Recently, the new technologies used by different actors over the internet challenge privacy in new complicated ways that did not exist before. Governments and tech companies use artificial intelligence to gather private

[6] Global digital population as of January 2021, https://www.statista.com/statistics/617136/digital-population-worldwide/.

[7] Number of internet users worldwide from 2005 to 2019, https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

[8] Brittainy Cavender, The Personalization Puzzle, 10 Wash. U. Jurisprudence REV. 97 (2017), at 97.

information and know more about one's interests, habits, economic level, and political thoughts. The addiction to social media pushed people to abandon their privacy in dangerous ways. In order to benefit from an application, people agree on the terms and policies without even reading them. Tech companies exploit this advantage for their interest by collecting more data. Most people would not realize the threat of revealing a small piece of data. They even do not understand that just scrolling down the screen on Facebook or Instagram may reveal important information about the user's personality that he/she may want to hide from others. The new systems stalk every and each one uses a device that is connected to their websites or applications. They restore and analyze all gathered data in order to predict their behavior and maybe nudge people towards a specific path by shaping their ideas.

Advanced algorithms challenged privacy by their capability to aggregate small pieces of data. Tech giants use complex algorithms that can aggregate small pieces of data from multiple resources at different times. They can identify the user, even if each piece could not achieve this purpose by itself, and/or reveal sensitive information about the user that he/she does not want to disclose. Moreover, such algorithms are protected by trade secret law which immune those companies from any attempts to fully understand and study those technologies. Personal data could be used in manipulative ways by companies that lack transparency and are motivated by profit. They usually use data to "feed off consumers' and voters' raw emotions, racial or national identities, shopping preferences, party affiliations, and any other metrics they can gather online."[9] They do not aim to provide correct or useful information; instead, they aim to provide the most relevant information to the user.[10] Therefore, the collection of personal data through the internet can be a massive threat to the right to privacy.

The internet mechanism "not only feeds the taste for consuming the privacy of others; it simultaneously constructs such tastes."[11] The internet facilitates the methods to look at other's private affairs. Most users post personal information about themselves, friends, and families on social media. They refresh their timeline multiple times to update the news;

[9] Alexander Tsesis, Marketplace of Ideas, Privacy, and the Digital Audience, (2019), at 1603.

[10] Cavender, supra note 8, at 107.

[11] Anita L. Allen, Coercing Privacy, 40 WM. & MARY L. REV. 723 (1999), at 735.

they access the profile of others to know more about them. Moreover, many people do not care about privacy and want to gain money and celebrity. In order to attract more followers and likes, women show their bodies; couples publish their love stories; husbands and wives share their daily activities. These challenges make many claim the extinction of the right to privacy as Facebook founder Mark Zuckerberg says that privacy is no longer a social norm.[12]

On the contrary, people around the world are concerned about their privacy over the internet. New surveys show an increase in online privacy concerns. In Egypt, 76% of internet users were concerned about their online privacy in 2019 than they were in 2018.[13] About 53% of all users around the globe also worry about their online privacy.[14] Moreover, the instance of changing WhatsApp privacy policy shows that internet users are still caring about their privacy over the internet. In January 2021, WhatsApp declares that it will change its privacy policy in order to share users' data with Facebook. Each user has to accept the new terms, or he/she will have no right to use the application. However, this step caused an enormous global reaction. Millions of users abandoned WhatsApp. Signal and Telegram, who claim that they have better privacy policies, see a surge increase in the number of users.[15] Accordingly, WhatsApp changed its position and delayed the application of the new amendment.[16]

B. Methods of Data Collection:

Users disclose their personal data while using the internet, whether explicitly or implicitly.[17] On social media platforms, users intentionally add their names, pictures, emails, status to their profiles on social platforms or other websites in order to be seen by

[12] Bobbie Johnson, Privacy no longer a social norm, says Facebook founder, the Guardian, https://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

[13] Share of internet users who are more concerned about their online privacy compared to a year ago as of February 2019, by country, https://www.statista.com/statistics/373322/global-opinion-concern-online-privacy/.

[14] Id.

[15] WhatsApp loses MILLIONS of users to rivals Telegram and Signal amid fears of increased data sharing with Facebook, Daily Mail, https://www.dailymail.co.uk/sciencetech/article-9183553/WhatsApp-loses-MILLIONS-users-rivals-Telegram-Signal-ahead-privacy-policy-update.html.

[16] WhatsApp delays privacy update over user 'confusion' and backlash about Facebook data sharing, CNBC, https://www.cnbc.com/2021/01/18/whatsapp-delays-privacy-update-amid-facebook-data-sharing-confusion.html.

[17] *See* Barbara Sandfuchs, Andreas Kapsner, Coercing Online Privacy, I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY 185 (2016).

their friends or other users generally. In order to benefit from online services, websites and applications ask a user to fill out a form that usually asks for personal data like name, age, gender, home address, zip code, email, job, telephone number, and other kinds of data according to the offered service. In other instances, the user may need to reveal sensitive information like health records or bank accounts. On the other hand, users have to accept the terms of a newly installed application, which grants the application the right to collect different data types such as IP address, operating system information, hardware model, and mobile network information. ISPs track and record users' online activities like shopping habits, location, the posts and people you view or engage with, the time-frequency, and the duration of using the app. They even may track users' activities when they are offline. For example, Google admits that it collects users' location from Android phones even if the device is offline or does not have a SIM card.[18]

Websites and applications commonly use cookies to document users' activities. Cookies are a very small piece of data that enables the site to record the users' activities and browsing patterns in order to identify the user each time he/she visits the website and enhance the user's experience by showing the choices that match with his/her preferences.[19] Before issuing the European general data protection regulation (GDPR), websites placed cookies on one's computer without even notifying her. Thanks to the GDPR, most websites ask or notify the user that they use cookies. In addition, some websites share their cookies with third-party or allow them to put their own cookies on users' devices through the website directly.[20] Furthermore, many programmers use the 'beacon,' or 'Web bug,' which enables live surveillance of user's online activity on a website, "including where one's mouse moved and the information that one typed, such as search queries or personal information that an individual filled into a form."[21]

[18] Shannon Liao, Google admits it tracked user location data even when the setting was turned off, The Verge, https://www.theverge.com/2017/11/21/16684818/google-location-tracking-cell-tower-data-android-os-firebase-privacy.

[19] Dr Anan Sh. Younes, Passive Violation of Consumers' Privacy Rights on the Internet in the Age of Emerging Data Capital, 10 Journal of Content, Community & Communication 134 (2019).

[20] Id. at 136.

[21] Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. REV. 1814 (2011), at 1851.

Moreover, the Internet of Things (IoT) is another source that allows tech companies to consume more personal data. It is a system that connects objects and gadgets with the internet in a manner that allows the collection and transfer of data without human intervention. It is used, for example, in home appliances, cell phones, cars, and security devices. In order to function, the system gathers data about the user and his/her activities.[22] In some instances, it has to watch and record the user's voice, face, live actions. Appliances equipped with sound systems and/or cameras can record every sound and movement in the house. Those data are transmitted to the servers of the manufactured company, which would use them to study their users. Consumers, however, would not know the actual usage of their data.

C. Problem Roots:

Governments and tech companies use artificial intelligence to gather private information and to know more about one's interests, habits, economic level, and political thoughts. Algorithms can reveal sensitive information by aggregating information that is posted online on different websites over a long period of time. Moreover, the addiction to social media pushed people to abandon their privacy in dangerous ways. In order to benefit from an application, people agree on the terms and policies without even reading them. For example, a study shows that only three percent of users read privacy policies.[23] Tech companies exploit this advantage for their interest by collecting more data. Most people would not realize the threat of revealing a small piece of data. They even do not understand that just scrolling down the screen on Facebook or Instagram may reveal important information about the user's personality that he/she may want to hide from others. The new systems stalk every and each one uses a device that is connected to their websites or applications. They restore and analyze all gathered data in order to predict their behavior and maybe nudge people towards a specific path by shaping their ideas.

The main cause of online privacy violations is the relentless pursuit of gathering data, whether by private or public actors. Statistics show the increasing users' concerns regarding their online privacy, but their online activities prove the opposite; many people seem that they do not really care about their privacy. However, the question is why those actors are

[22] Tsesis, supra note 9, at 160.

[23] Younes, *supra* note 19, at 143.

so greedy to know more about other people. The literature reveals that tech companies and governments are motivated by economic and political incentives, while users are willing to disclose their personal information for social motives.

1. Commercial Incentives:

"*The world's most valuable resource is no longer oil, but data*."[24]

- Economist, 2017

Technology companies realize the value of data and its importance for their growth. Tech giants like Facebook and Google gain billions of dollars from selling advertisements. For example, Google's revenue amounted to a total of 181.69 billion US dollars; mostly 146.92 billion US dollars are from selling ads in 2020.[25] Moreover, purchasing goods and services online has become one of the most popular online activities worldwide. In 2016, 1.66 billion people bought goods and services online; this number is mounted to reach over 2.14 billion digital buyers, in 2021.[26] In 2020, retail e-commerce sales amounted to 4.28 trillion US dollars and e-retail revenues are projected to grow to 5.4 trillion US dollars in 2022.[27] The massive increase in revenues reflects the value of Big Data. Therefore, tech companies are too greedy to know more about users because the more they collect data, the more they profit, which makes personalization inevitable.

They spend a huge amount of money and time developing algorithms that can attract more users and analyze the data collected in order to know more about their users. They analyze users' personal information, searches, likes, clicks, and even the time they spend looking at a post or video.[28] They change the architecture of their programs to attract more users and make them spend more time on their applications because the more they stay online, the more they collect data and understand consumers, the more they can sell ads and boost their revenues. Facebook, for instance, admits that they aim to make users more

[24] The world's most valuable resource is no longer oil, but data, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[25] Advertising revenue of Google from 2001 to 2020, https://www.statista.com/statistics/266249/advertising-revenue-of-google/ (As of October 2020, Google holds a market share of around 90 percent in a wide range of digital markets.).

[26] Number of digital buyers worldwide from 2014 to 2021, https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/.

[27] Retail e-commerce sales worldwide from 2014 to 2024, https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

[28] Cavender, supra note 8, at 105.

addicted to their app.[29] Friendster, an American tech company, holds a patent on a "Method of inducing content uploads in a social network."[30] Many companies provide social media platforms with algorithms that aim to attract more users or spend more time on their apps. Tech companies categorize the users and create a personal profile for each one in order to personalize the posts, articles, videos, and advertisements that will appear on each user timeline, which increases their revenues by selling more ads. They will show up the most relevant results for the user based on his/her behavior.

In the current era, behavioral marketing has been replaced mass marketing. Marketers for a long time have resorted to publishing ads in newspapers or televisions; they aim to aware the public in general of their products. However, behavioral marketing proved its efficiency in digital marketing. It duplicates the return from investment from five to eight times.[31] Marketers can target consumers based on their location, revenue, sex, and/or habits. They target the classes that would probably buy their products and services. For example, while an Egyptian user who visits independent.co.uk would see ads from Egyptian companies for goods that match his/her preferences, a German visitor would see other advertisements that match with him/her on the same site. Even if they are from the same neighborhood, they would see different ads. Instead of selling ads for newspapers, television, and websites, "advertisers now seek to buy access to individuals who fit a certain profile."[32] Tech companies are commodifying users and selling users' profiles to advertisers. They shift their focus from users to marketers and revenues.

The eagerness to collect data attracts more investments in the Business Analytics Market. They work on new methods that can analyze a tremendous amount of data in order to convert those data to "actionable knowledge."[33] They provide the decision-maker with the best decisions. In 2020, this business valued 67.92 billion US dollars and is expected to reach 103.65 billion US dollars by 2026.[34] Due to the positive expectations, more

[29] Olivia Solon, Ex-Facebook president Sean Parker: site made to exploit human 'vulnerability', The Guardian, https://www.theguardian.com/technology/2017/nov/09/facebook-sean-parker-vulnerability-brain-psychology.
[30] James Grimmelmann, Saving Facebook, 94 IOWA L. REV. 1137 (2009), at 1156.
[31] Younes, *supra* note 19, at 142.
[32] Schwartz & Solove, *supra* note 21, at 1851.
[33] *Id*.
[34] BUSINESS ANALYTICS MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2021 - 2026), https://www.mordorintelligence.com/industry-reports/global-business-analytics-market-industry.

companies have specialized in the new business. Those companies do not serve only economic entities but also political parties.

2. **Political Motives:**

Governments seek to exploit the data for political reasons. They hire analytics companies to analyze people's behavior in other countries and nudge them into a specific direction. In the US 2016 presidential election, many scholars discussed the Russian attempt to influence the American people and manipulate the election.[35] Some Russian officials created fake accounts on social media and used them to post thousands of misleading messages to manipulate public opinion by promoting racial and social divisions.[36] They purchased thousands of ads from Facebook that target special groups based on their jobs, location, and racial and social interests.[37] Meanwhile, the Trump campaign linked to the misuse of over 87 million Facebook users' profiles leaked to Cambridge Analytica.[38] The campaign used those data to build voters' profiles which permit to influence the 2016 election's result.[39] There are also other allegations regarding the role of Cambridge Analytica in influencing the Brexit vote.[40] Therefore, personal data gathered by tech companies could jeopardize democracy and manipulate people's minds.

Moreover, police and armies buy personal data from third parties in order to monitor and surveille people. In 2020, it was revealed that the American army bought the location of Muslim Pro users that has been downloaded almost 100 million times. Muslim Pro sold the data to a third-party broker called "X-Mode," who sold them to the American military.[41] They use that data to plan and execute military operations.[42] Even though the company claims that those data are anonymized, some studies proved that it could be easily de-

[35] See William J. Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 24 MICH. J. RACE & L. 177 (2019).

[36] Id.

[37] Id.

[38] Sarah Shyy, The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy &Significant Burdens on Business, 20 U.C. Davis Bus. L.J. 137 (2020), at 138.

[39] Nicholas Confessore, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, The New York Times, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[40] Id.

[41] Aaron Holmes, The US military reportedly bought location data mined from a popular Muslim prayer app to track users for 'counterterrorism', Business Insider, https://www.businessinsider.com/us-military-location-data-muslim-prayer-app-xmode-babel-street-2020-11.

[42] US military is buying location data from popular Muslim apps, Tribune, https://tribune.com.pk/story/2272573/us-military-is-buying-location-data-from-popular-muslim-apps

anonymized by connecting that piece of data with other data that can be collected from other sources.[43] In addition, some companies used available sources on social platforms "to monitor "protest groups and marketed that data to police departments."[44] Those are some examples that show the massive power and capabilities that governments can have if they acquire the personal data collected.

In the Middle East, the role of social media platforms grabbed the attention of Arabian countries since the 2011 "Arab Spring."[45] People used Facebook and Twitter extensively to spread the news of the revolution. However, governments observed and learned from this experience. They create and use thousands of fake accounts to attack opposing opinions; they block and report opposing accounts. Moreover, the Egyptian government has issued personal data protection law No.151 for 2020, which organizes the personal data issue similar to the GDPR. The Egyptian law established a new entity that will have the power to organize, inspect, and license the data collection and processing. The entity board will be constituted of representatives of the military, police, and ministry of communications. Such power can be misused to surveil people and intervene in their private life as what happens in other nations.

3. Users' Motives:

Commercial and political entities could not obtain those vast amounts of data without the users' cooperation. Although one can understand the motives of commercial and political entities to collect personal data, the position of most users is questionable. Those entities could not collect those data without the contribution of users, whether explicitly or implicitly. So, why do users underestimate the privacy risks? Why do they abandon their privacy in such dangerous ways?

People want to benefit from the available information and knowledge on the internet. It provides many people a vast amount of information about almost everything in life. They can learn new skills, read books, and conduct researches. if one wonders about something unknown, the advice will be "Google it!" Google can answer whatever question one's has,

[43] Stuart A. Thompson and Charlie Warzel, Twelve Million Phones, One Dataset, Zero Privacy, The New York Times, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html
[44] Tsesis, *supra* note 9, at 1606.
[45] Peter Swire, Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment, 90 N.C. L. REV. 1371 (2012), at 1373 (mentioning the role of Facebook in the Egyptian revolution in 2011).

despite the accuracy of the provided information. Moreover, people, especially new generations, get used to using the internet, whether websites or applications, to do the shopping and get services. In order to benefit from the internet, they have to accept the terms and conditions of the service provider and give away personal information. Meanwhile, users lack knowledge about the possible ways to protect their personal information on their devices. People are not aware of the risks of privacy erosion; they follow other users that did so before. In other words, "When our friends all jump off the Facebook privacy bridge, we do too. Those behind us figure we wouldn't have jumped unless it was safe, and the cycle repeats."[46]

On social media platforms, users disclose their personal data for social reasons. People reveal important data, such as pictures, emails, status, opinions, while using social media in order to attract more friends and followers. Prof. Grimmelmann demonstrates Facebook users' motives to disclose their personal information: "Facebook provides users with a forum in which they can craft social identities, forge reciprocal relationships, and accumulate social capital."[47] Social media platforms fulfill the social needs of their users.[48] First, social networks permit users to say who they are. They construct their identity through the posts and information they say about themselves. They try to impress and convince other friends or the public to accept their claims about who they are, how they look and live, and what are their standards and hobbies.[49] Secondly, social media platforms give a chance for a user to make new friends and deepen the relationship with current ones.[50] A user interacts with others and shares posts and stories about him/herself, family, friends to deepen the friendship. Finally, people aim to establish a social position within the online community through their profiles on social media. They want "to be recognized as a valued member of one's various communities."[51] People join Facebook because their peers and friends joined early. They want to join that social community, or they would feel lonely and eliminated. They also have to add more friends to their profiles in order to be

[46] Grimmelmann, *supra* note 30, at 1161.
[47] Id., at 1151.
[48] Id.
[49] Id., at 1152.
[50] Id., at 1154.
[51] Id., at 1157.

more visible within the online society. These social motives explain why people systematically underestimate the privacy risks over social networks.

III. Informational Privacy

A. Privacy is Everything and Nothing:

Privacy right is a fundamental right for each citizen in society. As Anita L. Allen described it: "[p]rivacy is not an optional good, like a second home or an investment account."[52] A citizen needs a private sphere to act freely without any intervention or surveillance. The state protects this space by several legal rules, such as the prohibition of unlawful surveillance, unwarranted search and seizure, intrusion, defamation, and disclosure of sensitive information that was shared with a trusted one, like health records. One should have the right to control the time and the manner of revealing or share his/her body, ideas and information with others, to prevent the dissemination of these types of information, whether they are true or false, and to correct the false ones. Being exposed without prior consent would threaten this sphere.

Moreover, worrying about being watched by public or private parties would undermine his/her ability to innovate and participate in public debates. Individuals generally need a comfortable area to talk and discuss public policies. As Julie E. Cohen stated, privacy is "foundational to the practice of informed and reflective citizenship."[53] In order to have a healthy society based on values like respecting the other and encouraging pluralism, innovation, and healthy debates, the state has to secure an environment to flourish. Citizens have to be well informed and have access to different opinions in order to achieve a reasonable decision. Protecting such rights is managed by different legal rules because privacy is a value that could not be compressed in one law.

Although the fundamental role of privacy right in the life of individuals and societies, privacy does not have a clear definition in the mind of ordinary people or even some scholars. Unlike rights like the right to life, freedom of expression, and health, privacy is too vague to define, but it exists in many aspects of life. As Prof. Solove summarized it: "[p]rivacy seems to be about everything, and therefore it appears to be nothing."[54] Privacy right suffers from the lack of comprehensive definition because it intersects with multiple

[52] Allen, *supra* note 11, at 740.

[53] Julie E. Cohen, What Privacy is For, 126 HARV. L. REV. 1904 (2013), at 1905.

[54] Id.

rights.[55] It is an "umbrella term" that encompasses wide and different categories of rights.[56] It is related, for example, to the right of freedom of expression and thought, human dignity, health and welfare, autonomy and self-determination, and freedom from surveillance, illegal search, and interrogation. Therefore, privacy law is always seen as ineffective because of the challenges "in articulating what privacy is and why it is important."[57]

Privacy is a right of an individual who lives within society. The concept assumes that there is a public sphere that exists besides the private one, and there is a distinction between them. Privacy cannot exist without a society because there would be no need for it if individual lives alone on a remote island. It is essential for each individual in every community to have a private sphere, but this sphere's dimension is not the same in each society. Society's values and culture affect the scope of the right. Nonetheless, the individual self-understanding of the meaning of privacy might vary within the same society according to "one's generation, educational background, and wealth."[58] However, privacy could not basically depend on an individual's expectations and thoughts because it could lead to the demolition of privacy. Individuals' expectation of privacy is already shrinking in the current era due to the expanding use of the internet and new technologies. Governments could gradually enforce the acceptance of surveillance which would diminish their expectations of privacy. Nevertheless, privacy could not be a block of activities that are protected all the time because it will fail to catch the rushing evolvement in the modern world. Therefore, privacy is an elastic concept that simultaneously reflects individuals' and society's beliefs and standards and affects them.

The foundation of the privacy law has been raised, for the first time in American history, by Samuel Warren and Louis Brandeis in their famous article "The Right to Privacy" in 1890.[59] They called for nonintervention of the press in one's private affairs and the right of an individual to be "let alone."[60] The article emerged a debate over the scope and the limitations of the application. Some scholars noted that the previous definition was

[55] Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477 (2006), at 477.
[56] Id.
[57] Solove, *supra* note 2, at 1090.
[58] Allen, *supra* note 11, at 736.
[59] James H. Barron, Warren and Brandies, the Right to Privacy, 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation, 13 Suffolk U. L. REV. 875 (1979).
[60] Id.

too broad because privacy violations could include any unwelcome act.[61] As Prof. Allen described it: "[a] punch in the nose would be a privacy invasion as much as a peep in the bedroom."[62] In 1960, the famous tort scholar William Prosser identified four types of privacy invasion in his article "Privacy."[63] Even though Prosser's contribution significantly develops the legal framework of privacy, his effort focuses only on tort law. Privacy is more complex, and it extends to many other legal fields like trespass, wiretapping, illegal search and seizure, and informational privacy. Moreover, the internet and social media challenged privacy in a manner that did not exist before. Scholars like Warren, Brandeis, and Prosser reflected on a world that massively changed.

In Egypt, privacy right did not have enough legal attention till the last few years. The old versions of the Egyptian constitution protect an individual's body, correspondences, and home from unwarranted search or seizure. Courts generally apply this rule in criminal cases like the possession of drugs and guns. In 1995, the constitutional court declared that every individual has the right to hide some aspects of his/her life.[64] It is always necessary to ensure and preserve their confidentiality and to prevent any attempt to spy or violate them, the court added. After referring to the American legal system, the court emphasized the impact of the astonishing characteristics of new scientific methods which allow the hacking of private life and getting access to private matters and personal data. In addition, the penal code criminalizes the violation of private life by prohibiting the recording, transferring, and dissemination of private calls or pictures.[65] In 2014, the Egyptian constitution provided the protection for private life while stipulated the prohibition of the wiretapping of *electronic* correspondences for the first time under article 57.[66] In 2018, Egypt issued the Anti-Information Technology Crimes Law No. 175 for 2018, which criminalizes many kinds of cybercrimes. Article 25 of this law prohibits the usage of online

[61] Solove, *supra* note 2, at 1102.

[62] Id. (cited Anita L. Allen, Uneasy Access: Privacy for women in a free society 7 (1988)).

[63] William L. Prosser, Privacy, 48 Cal. L. Rev., Aug. 383 (1960), (The four types of invasions are: (1) intrusion upon the plaintiff's seclusion or solitude or into his private affairs; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity which places the plaintiff in a false light in the public eye; and (4) appropriation for the defendant's advantage).

[64] 23 for 16 in 18/3/1195, Constitutional Court.

[65] Penal Code article 309 duplicated, and 309 duplicated A.

[66] Constitution Of The Arab Republic of Egypt, 2014.

tools to violate one's privacy.[67] Even though article 25 wording is too general to encompass all activities that would violate the user's privacy, the Egyptian courts need more time to elaborate their interpretation for the scope of its application.

B. What is Informational Privacy?

Putting an inclusive short definition of privacy seems an unreachable objective. Privacy invasion can damage various kinds of standards, customs, and norms, which could not be encompassed in one sentence. Prof. Solove, in his article "Conceptualizing Privacy," tried to identify all privacy invasion practices and classified them into the following classes: (1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy.[68] These headings include the privacy invasion against one's body, home, and information. However, my research focuses on privacy invasion over the internet, which deals with informational privacy only, including the collection, processing, distribution, and dissemination of data.

In this paper, I aim to define informational privacy by identifying the various types of harms that affect a user and/or a society through data invasion activities. I would try to identify the online activities that cause troubles to users and societies. Indeed, privacy harms would not necessarily mean illegal acts, in my analysis. In other words, harm can be resulted out of either legal or illegal acts. Thus, for the purpose of this paper, harms mean any activity that causes troubles to an individual or a society or increases the risk of.

I clarify the online activities that cause privacy problems, which might be found in different fields. Privacy violations might cause, for example, reputational injury, lack of respect, and emotional and material harm. Privacy violation would make people feel vulnerable; such a feeling might force many people to alter their behavior. Further, privacy right provides the protection against breach of confidentiality, illegal searches of person or property, damage caused from stealing personal information like identity theft and fraud, invasion of solitude, and surveillance. Meanwhile, Solove, in his article "A Taxonomy of Privacy," builds a taxonomy based on the harms that affect the user only while there are other aspects of harms that affect the society overall. I develop Solove's taxonomy of

[67] Law No. 175 of 2018 (Law of Anti-Information Technology Crimes).

[68] *See* Solove, *supra* note 2. (Those classifications include: The right to exclude others from (a) watching, (b) utilizing, (c) invading private affairs; The right to keep some information secret. The right to control how, when, and to what extent personal information is collected or disseminated.)

privacy by elaborate his classification and add a new classification regarding the harms that affect society. Thus, a successful definition of privacy needs to identify all kinds of activities that involve privacy invasion and cause problems to data subjects and societies.

By adopting that perspective, I aim to achieve multiple results. First, I emphasize the significance of privacy in an individual's life and society and the harms that affect a user or a society from privacy violations. Second, such a demonstration would help to differentiate between the negative and positive aspects of treating the data by different stakeholders. Finally, such differentiation is vital to identify the role of law in dealing with that problem because a policymaker needs to prevent harmful actions while promoting non-harmful ones.

1. Harms to Data Subjects:

In the cyber world, personal data go through three phases: collection, processing, and dissemination. First, the information collection phase is concerned with the method of gathering the information, such as surveillance and interrogation. Then, the data holders would process those data, which involves the ways of handling the collected information. It deals with the storage, usage, and manipulation of the data. The final stage is dissemination, which is concerned with the transfer of data. Each phase implies certain types of harm, as I demonstrate in the following points.

i. Data Collection:

The first step is collecting data which can be done in various ways, as I demonstrated earlier. However, the methods of collection imply harm because they represent surveillance and interrogation. Surveillance means that someone is listening, watching, or recording a person's actions. In order to collect data, tech companies observe and record each click, search and mouse move on the screen that are done by every single user. Such behavior is prohibited for government agencies unless they have a judicial warrant. Law protects citizens from these practices because they would feel anxious and uncomfortable in a way that can force them to alter their behavior. It is used to guide and control the behavior of people because people give more attention to their behavior if they are being watched by others.[69] Such power would harm an individual's freedom and creativity and destroy his/her peace of mind, as professors Cohen, Solove, and Schwartz observed.[70]

One could argue that most users are not aware or notice that their online activities are being recorded. Even though the awareness of being watched is what affects one's behavior, the awareness of the *possibility* of surveillance could lead to less willingness to contribute in public debates or alter the way individuals engaged with as it does with the panopticon's prisoners.[71] Moreover, collecting a vast amount of data through surveillance might cause abuse of power because it can reveal sensitive information which could be used in illegal activities like blackmailing, for example.

On the other hand, data collection implies an interrogation process which means that people are feeling coerced to disclose their data. A user has to give out her personal data and accept the terms of conditions in order to benefit from the online services. In most cases, if a user refuses to grant the application access to his contacts, pictures, and location, he would not be able to finish the installation of the app. People could not bear the feeling of deprivation from the benefit of the internet. Moreover, social media create worries about users' image in the eyes of other members of the community. A user has to reveal some personal information to create a certain impact in other users' minds. Therefore, the collection process would coerce people to reveal more data and would make them worry about handling those data.

ii. Data Processing:

After collecting the data, the data holders process it, which includes its storage, usage, aggregation, and security. First, one of the duties of the data holders is guarding the collected data. They have to secure the data from leaks, hacking and improper access in order to protect their commercial interests in the data. Otherwise, they would lose the trust

[69] Solove, *supra* note 55, at 493. Mentioning John Gilliom observation: "Surveillance of human behavior is in place to control human behavior, whether by limiting access to programs or institutions, monitoring and affecting behavior within those arenas, or otherwise enforcing rules and norms by observing and recording acts of compliance and deviance." Citing JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY 3 (2001).

[70] *See* Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 STAN. L. Rev. 1373, 1397-98 (2000), at 1426; Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 VAND. L. REV. 1609, 1611 (1999), at 1656; Solove, *supra* note 2, at 1130.

[71] Solove, *supra* note 55, at 495. (This phenomenon called the Panoptic effect which based on observation that prisoners would adhere to the prison's rules because it is possible that they are watched even though they do not see the guards.)

of their users. However, a big data breach happened in the last few years. In 2018, over 9 billion data points were leaked from Apollo. In 2013 and 2014, over 3.5 billion users have been affected by two hacking attempts on the Yahoo platform.[72] Those data have been used in committing crimes like identity theft and fraud. It could be manipulated and used in extortion and blackmailing also. Meanwhile, revealing sensitive information could harm one's reputation because revealing the negative information in her financial or health records, for example, would cause embarrassment. The revealing of collected data would affect not only the data subject but also her family, friends and colleagues because the data usually involves information about others.

One of the astonishing characteristics of new algorithms is the ability to combine various pieces of data, which raises many privacy concerns. New technologies can gather small pieces of data that have been revealed on various websites at different times, which is known as "aggregation." Tech companies use this feature to analyze their users' behavior and generate the most relevant results for them. However, this characteristic could lead to substantive harm by revealing private information. Aggregation could lead to the revealing of sensitive or private information that a user did not intend to disclose it or share it with the data holder. Moreover, in many cases, people reveal some data because they assume that they would be anonymous. Nevertheless, aggregation could identify the user. User identification could jeopardize the ability to express her ideas and criticize the employers she works for because people tend to talk freely when they hide behind a pseudonym. It would also threaten users' access to non-biased news and ads that target them based on their identities.[73]

Data usage could also injure informational privacy. While data subjects disclose personal information aiming to benefit from certain advantages, data holders use those data, supposedly, for certain purposes related to their businesses. However, the data market shows that data are being used without the user's consent "for purposes unrelated to the purposes for which the data was originally collected."[74] This process is commonly known as "secondary use." These kinds of usage could create several types of harm. In the pre-

[72] Number of compromised data records in selected data breaches as of January 2021, https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/

[73] Solove, *supra* note 55, at 515.

[74] Grimmleman, *supra* note 30, at 1169.

mentioned example, over 100 Muslims' personal information were sold to the American army without their consent. Data traders are commodifying our personal data. They ignore users' right to control their personal data, which leads to an asymmetry of knowledge problem.[75] People worry about how their information are used, which creates a feeling of powerlessness and vulnerability.[76] Moreover, removing the data from its context could lead to distortion and manipulation. The third-party can buy and use the data in a manipulative way that would harm the data subjects, as happened in the 2016 US presidential election. Finally, such practices diminish the transparency and accountability of data holders because they fail and ignore to inform the users about how the data is used.

iii. **Data dissemination:**

Data dissemination involves the transfer or spreading of collected data to others which includes the breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion. People want to keep secret information that makes them vulnerable or can be used against their interests. However, the data can spread in cyberspace without the user's consent in a way that can harm him/her. The dissemination of *confidential and/or sensitive* information constitutes a privacy violation because the data subject has a legitimate interest in hiding some kinds of information away of the public. Likewise, *exposing one's nudity, grief, or bodily functions* would injure his/her dignity and create embarrassment and humiliation.[77] Similarly, the disclosure *of truthful information*, as long as the user did not want to disclose it, may cause reputational damage, especially if that information "is not of legitimate concern to the public."[78] Meanwhile, spreading *false information* would constitute defamation which injures one's reputation. Moreover, the dissemination of information amplifies the accessibility of information and deepens the harms. Spreading harmful facts or false information on the internet has a huge impact on the concerned person due to the ability of the internet to spread the information fast and the hardness in removing or correcting the disseminated data. Finally, data dissemination

[75] Schwartz, *supra* note 70, at 1683. "[I]ndividuals are likely to know little or nothing about the circumstances under which their personal data are captured, sold, or processed. This widespread individual ignorance hinders development through the privacy marketplace of appropriate norms about personal data use. The result of this asymmetrical knowledge will be one-sided bargains that benefit data processors."

[76] Solove, *supra* note 55, at 522.

[77] Id., at 536.

[78] Id., at 530.

expands the threats of committing crimes like blackmailing and identity theft by hacking tech companies' servers or users' devices. It opens the door for manipulation and distortion of the data in harmful ways to the users.

2. **Harms to Society:**

Privacy is not important for individuals only but also for societies. Many scholars describe privacy as a constitutive element of society.[79] A civil democratic society needs to provide protection against privacy invasion for its citizens in order to works properly. Privacy violations would increase the polarization, affect the individuals' cognition, and allow third parties to manipulate them to shape their beliefs and nudge them towards a specific direction.

Privacy harms to society have been created through the personalization process. Social media platforms and tech giants watch, record, and analyze every like, share, and move in order to identify user's preferences; they use the collected data to build a profile for each user. Then, the system will begin to show up the most *relevant* posts, news, and videos that confirm user's beliefs and biases which creates "*echo chambers*."[80] As professor Lessig observes: "The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is fed back to you in the form of options set by the pattern; the options reinforce the pattern; the cycle begins again."[81] The echo chambers phenomena have severe effects on society.

Even though such applications aim to provide users with the best experience that encourages them to find what they want easily and quickly, the users fall into feedback loops that isolate them from different ideas and opinions and impede their access to unbiased information, which threatens the freedom of speech and democracy. A citizen needs unbiased and unrestricted access to information in order to shape a balanced opinion.[82] She has to read different and opposing arguments to evaluate which point of

[79] See Solove, *supra* note 55, at 488 – 489 ("privacy harms affect the nature of society and impede individual activities that contribute to the greater social good."); See Cohen, *supra* note 70, at 1427-1428 ("Informational privacy, in short, is a constitutive element of a civil society in the broadest sense of the term."); Schwartz, *supra* note 70, at 1613 ("[I]nformation privacy is best conceived of as a constitutive element of civil society.").

[80] *See* Cavender, *supra* note 8.

[81] Lawrence Lessig, Code: Version 2.0 220 (2006).

[82] Cavender, *supra* note 8, at 114.

view is more valid. However, algorithms will show only results that match with the user's biases and isolate her from the contrary opinions and information, which feeds the polarization in the society.[83] Unlike traditional media, an individual would not be able to freely choose what to read; algorithms would decide what to hide and what to show up. In other words, a user could not read a post or watch a video that would not show up on her screen. Meanwhile, reading repeatedly similar opinions creates an impression that this idea is a fact and blocks individuals' minds from the contradictory opinions of their fellow citizens. Therefore, the echo chambers would jeopardize the achievement of healthy public debates.

Moreover, those algorithms can be abused by tech companies and governments to shape users' beliefs and nudge them in a specific direction. The content that users see contributes in shaping their identities and thoughts, as I discussed earlier. In the meantime, truth seems a hard objective on the internet because algorithms do not detect the accuracy of the information. Tech companies, governments, and individuals can use this feature to manipulate people's cognition and nudge them towards their political or commercial objectives. They would amplify fake news and mistrusted information which can "make individuals vulnerable to believe falsehoods."[84] It is easy for corporates and governments to create thousands of fake accounts and buy target ads to shape people's beliefs. The 2016 US presidential election shows how a foreign government can use personal data to manipulate with people's minds in order to serve its interest.[85] Therefore, the erosion of privacy is a real risk for the development of individuals and democracy within society.

3. PII and non-PII:

The previous illustration of privacy implies an assumption that an individual's right to privacy is protected as long as the data does not identify the data subject. Privacy harms that affect a user's reputation, dignity, and emotions could not be imagined unless the data reveals his/her identity. Tech companies argue that the collected data is anonymized, which would not threaten privacy. They restore and transfer data without identifying the user's name. They build a profile for each user that contains his/her data, but they exclude the

[83] *See generally* Cass Sunstein, REPUBLIC.COM 2.0 (2007).

[84] Sofia Grafanaki, Drowning in Big Data: Abundance of Choice, Scarcity of Attention and the Personalization Trap, a Case for Regulation, 24 RICH. J.L. & TECH. 1 (2017), at 19.

[85] *See generally* Aceves, *supra* note 35.

personally identifiable information (PII); they give a code for each profile, instead.[86] They aim to track the user's activities, not to reveal his/her identity. As a result of their argument, most of the collected data is non-personally identifiable information (non-PII) which falls outside the scope of privacy regulations.

The differentiation between PII and non-PII is problematic. Many people believe that most of their online practices are anonymous. They believe that no one can identify their persons unless they intentionally reveal their identity. However, online anonymity is a myth.[87] Many scholars pointed out data can be deanonymized by triangulating indirect information.[88] Algorithms can combine various pieces of data, which would consequently reveal the user's identity. For example, a study shows that 87% of Americans can be identified by combining a ZIP code, sex, and birth date.[89] Paul Ohm suspects even the existence of that differentiation because most non-PII can be re-identified, and data would lose its utility if they lack information that can identify the user, whether directly or indirectly.[90] Moreover, the evolvement of new technologies creates uncertainty in that field because programmers find new ways to combine different pieces of data and transform them into PII.

The GDPR and the Egyptian Anti Information Technology Crimes Law No. 175 for the year 2018 solved this problem by defining personal information as any information that can identify a person, *whether directly or indirectly*. This definition encompasses any piece of data that can identify a user identity by combination with other data collected by different parties on multiple occasions and times. I advocate this direction because revealing the user's identity by combining different pieces of data will threaten privacy more than direct disclosure. People depend on anonymity, even it is a myth, to act freely online. They do not expect and accept that their actions would identify them in person. Such expectations should be protected by law. Conversely, a user that fills in an application

[86] Schwartz & Solove, *supra* note 21, at 1854.

[87] See Id.; Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. REV. 1701, 1719 (2010).

[88] Tsesis, *supra* note 9, at 1606-1607.

[89] Schwartz & Solove, *supra* note 21, at 1842. (citing Latanya Sweeney, Simple Demographics Often Identify People Uniquely 1 (Carnegie Mellon Univ., Sch. of Computer Sci., Data Privacy Lab., Working Paper No. 3, 2000)).

[90] *See* Ohm, *supra* note 87.

to create a profile on Facebook knows and accepts that he/she discloses personal information that would be shared with others.

IV. Online Privacy Self-Management

Engaging with online privacy problem calls for a position regarding the dilemma of "self-management." Citizens are autonomous competent individuals. An individual has the right to act and choose freely in a *self-interested* manner as long as his/her actions do not harm other individuals.[91] The government should protect the freedom of each one from its own and/or other individuals' intervention. In other words, the government should not contest the autonomy of individuals by forcing them to act or refrain from a specific act unless this act causes significant harm to others. That contradiction between individual rights and state powers can be found in almost all aspects of life. Therefore, the law should regulate this contradiction by promoting the freedom of choice and simultaneously providing security from harm.

Due to the threats of privacy erosion, many scholars are trying to find a solution to this complicated problem. While some scholars advocate the coercion of privacy, others argue for the non-intervention of government. However, many countries adopt the user empowerment strategy by giving users a bundle of rights to control his/her personal data. In this chapter, I analyze the proposed legal solutions and show the gaps that they left in dealing with online privacy. Then, I demonstrate how Thaler and Sunstein dealt with the self-management dilemma by demonstrating the libertarian paternalism theory.

A. Evaluation of Different Legal Approaches:

1. Coercing Privacy vs. Do Nothing:

On the one hand, Anita L. Allen argues for coercing online privacy because the harms outweigh the benefits, which calls for government intervention to protect the people. She emphasizes the significance of privacy for the individual and society while showing how privacy threats jeopardize liberal values. Coercing privacy norms would protect individuals and societies. She claims that adopting regulations that aim to curb the exposure culture would enforce people to like privacy.[92] Meanwhile, one might argue that state should enforce the right to privacy by illegalizing the online activities that harm user's privacy. Accordingly, such policy would help to protect users' privacy.

[91] Singer, *supra* note 3.

[92] Allen, *supra* note 11, at 753.

However, coercing privacy is extremely difficult due to several reasons. Privacy coercion means that the flow of data will be impeded, which would affect almost every service on the internet because algorithms depend on data to operate. Internet services become essential in the life of millions of people as much as governments. They would be harmed if those services are stopped. In addition, data market is worth billions of dollars. Ecommerce, nowadays, is one the most important factors to the economy. Affecting the data market would affect the ecommerce which would hurt the economy overall. Meanwhile, tech companies have immense economic and political power, and they would use their powers to abort such laws that would severely affect their growth and reduce their revenues. For example, the congress failed to regulate the usage of data despite what happened in US presidential elections in 2016. Further, such coercion cannot be adopted by one state; it must be a collective work because tech companies would leave the state that put restrictions on collecting data and migrate to other countries that facilitate it, which will hurt its economy. Thus, governments and legislators will be so reluctant to adopt such coercive measures.

Moreover, online privacy is a very complex issue. Identifying which kind of data is allowed to be collected, processed, and disseminated is problematic. The context differs, which affects the final decision. Privacy while using social media is not the same as when visiting websites, for example. Algorithms complicate the issue by aggregating small pieces of data. A small piece of data, that is legally obtained, can be combined with other pieces, that are legally and independently collected on other websites. Such aggregation might reveal sensitive data that the user did not intend to reveal while using the internet. Furthermore, using a list of prohibited activities would not be effective because technology constantly develops in a way that laws could not catch up. on the other hand, prohibition some activities could breach other fundamental rights like freedom of expression and freedom of association.[93] People should have the right to speak freely and express their ideas without any limitations. Such obstacles will also limit people's ability to reach out others to create associations. Finally, coercion contradicts with individual's autonomy.[94]

[93] *See* Swire, *supra* note 45.

[94] Sandfuchs and Kapsner, *supra* note 17.

People should have the freedom to decide which data they want to disclose and which one they want to hide.

On the other hand, Barbra Sanfuchs and Andreas Kapsner argue for the non-intervention of governments. They claim that "governments are neither obliged nor allowed to prevent competent adult users from voluntary online self-disclosure by paternalistic interventions that only aim to protect the users."[95] While they refuse to impose any paternalistic measures to protect users, they advocate the promotion of self-management that aims to empower individuals to make their own decision without forcing users to act in a specific way. While I disagree with the idea of coercing privacy, doing nothing is ultimately the wrong answer because it would lead to more privacy erosion. Prof. Grimmlemann argues against resorting to market forces and "do nothing" because there is a market failure in the data market.[96] Users do not have power in the face of tech companies in order to bring some balance in the market, and therefore social media platforms will not be compelled to change their attitude.[97] Moreover, because behavior influences are inevitable, doing nothing means that governments surrender their citizens to commercial and political parties that manipulate them. Thus, a state role is needed to bring some middle ground in this issue.

2. User's Empowerment:

For a long time, tech companies try to self-regulate privacy in order to reassure their users. While some notice their users about their privacy policies, others ask for users' explicit approval before granting them the right to use their services. They promise their users that they will guard their data and protect their privacy. However, privacy policies did not give the user any power to bargain. A user has to accept the terms or would deprive of access. Meanwhile, governments noticed the risks from collecting, processing, transferring, and leak of personal data. They realized that they have to act to protect their citizens.

The European countries were the first to take a big step in regulating the data market. In 2016, the European Union issued the general data protection regulation (GDPR).[98]

[95] Id., at 185.

[96] Grimmlemann, *supra* note 30, at 1178-1179.

[97] Id.

[98] General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (27 April 2016).

Article 8 of the Charter of Fundamental Rights of the European Union gives all people "the right to the protection of personal data concerning him or her."[99] GDPR aims to protect natural persons with regard to the processing of personal data and regulate the movement of personal data. In order to achieve this goal, GDPR adapts several techniques that empower users. Article 15 gives the data subject the right to obtain from the controller the needed information about his/her personal data that have been collected. Article 16 allows the data subject to get rectification of inaccurate personal data concerning him/her. Article 17 creates the user's right to ask to be forgotten. In other words, he/she has the right to erase his/her personal data. Furthermore, the EU put some restrictions on transferring and storing data of EU citizens. For example, a data controller is obliged to maintain data protection-level and the records of data processing. Due to the EU economic and political power, most companies started to apply those rules.

Following the EU steps, Egypt issued its law for personal data protection No. 151 of 2020, which adapts similar rules that aim to promote privacy through empowering the Egyptian user.[100] Article 2 requires the explicit consent of the user before collecting or processing personal data. The new law grants the user almost the same rights granted in the GDPR, such as the right to be forgotten, to object, and to modify his/her personal data. The government aims to regulate the data market by imposing some duties on institutions that want to collect, hold, and process the data. They have to secure the data from any leakage or breach and appoint a responsible for it. They have to acquire a governmental license before doing any of the previous activities. Conversely to the GDPR, the Egyptian law does not require storing the data on its territory because Egypt does not have the technological infrastructure like large servers that can store such a big amount of data.

The GDPR and Egyptian law for personal data protection No. 151 of 2020 represent a significant development in the online privacy field. They aim to achieve a balance between the flow of data and the individual's right to privacy and a balance in power between tech companies and users. They decide to provide users with a bundle of rights that allow them to control their personal data. Under the current laws, users have the right to control what,

[99] Charter of Fundamental Rights of the European Union, EU: Council of the European Union C 303/1 (14 December 2007).

[100] Law No. 151 of 2020 (Law of Personal Data Protection).

how, when data can be collected or transferred and for how long data can be restored. They have the right to delete collected data and acquire information from data holders about their personal data. They refuse to coerce privacy while they chose to respect users' autonomy by empowering them.

However, the user's empowerment doctrine is ineffective in bringing the desired balance in the data market. There are several obstacles that hamper any attempt to empower fellow-citizens. First, many people are not aware of privacy risks or undermine those risks. Most data subjects could not foresee privacy risks due to the complexity of the data market. For example, surveys show that many Facebook's users do not pay attention to its privacy settings and others do not understand them.[101] They would not care about those rights as long as they do not believe in the threats. Second, as Prof. Allen underscores, commercial entities do "not only feeds the taste for consuming the privacy of others; it simultaneously constructs such tastes."[102] Accordingly, as long as tech companies are free to shape users' preferences, there will be little hope that a large number of users will pay attention to those rights. Thirdly, there are concerns regarding the capabilities of users to handle and exercise those rights properly. Users struggle to read all privacy policies, which brings shadows of doubt on their capabilities to evaluate the risks and decide which rights they want to activate. Even if they want to use those powers, they will not have the time or effort to do those calculations in each website and application they encounter in their daily usage. Furthermore, the "right of access" that is created by the GDPR has its own risks on privacy. It grants the user the right to know in detail what kind of data has been collected. What if someone impersonates the user? In a study, a researcher succeeded in collecting many personal information about his fiancé by impersonating her.[103]

Moreover, these laws disregard the privacy risks caused by other individuals. It is very hard to control the transfer of most data over the internet. Once the information is shared over the internet, it is almost impossible to erase it. If a user shares pictures and stories or sends messages via Messenger or WhatsApp, other recipients could take a screenshot or share that information with other persons. Such threats are not considered by the GDPR.

[101] Grimmelmann, *supra* note 30, at 1185.

[102] Allen, *supra* note 11, at 735.

[103] Shyy, *supra* note 38, at 159. (Citing JAMES PAVUR & CASEY KNERR, GDPARRRR: USING PRIVACY LAWS TO STEAL IDENTITIES (2019).)

One would argue that such practices are regulated by penal code or other laws. However, the collection and dissemination of data could be done in good faith by friends and family members, and its harmful effects cannot be foreseen in the short term. Finally, requiring the explicit consent of users on privacy policies would not cause a big difference "because consumers are still heavily pressured to agree to companies' data collection practices."[104] Rejecting the privacy terms means that the user would deny access to the website or the service he/she needs. This is a big burden that many users could not bear. Therefore, users' empowerment seems to be unsuccessful in encountering privacy risks.

On the other hand, the GDPR is burdensome for small businesses. It is applicable on all firms regardless of their size.[105] While GDPR exempts few entities in some circumstances from some duties, the Egyptian counterpart did not exempt any firms. Small businesses would suffer to adhere to new obligations because they do not have the same financial, technical, and human resources as large companies. In the EU, a company that has 500 employees has to spend three million dollars in order to comply with GDPR rules.[106] The costs include, for instance, hiring competent programmers to secure the data, executing compliance strategy, and legal fees. Such practices would impede the growth of small companies and new startups. New entrepreneurs will resort to other countries that have less strict laws.

In conclusion, the GDPR and the Egyptian law for personal data protection failed to achieve the needed balance in online privacy. They failed to promote privacy and to secure the data flow and business development. Data privacy is still far from a satisfactory solution.

B. A Libertarian Paternalism Entrance for Self-Management Dilemma

In the previous part, I demonstrated how the current legal approaches failed to deal with the online privacy problem. In my opinion, the libertarian paternalism theory provides a proper analysis of the self-management dilemma. In 2003, professors Sunstein and Thaler proposed the "libertarian paternalism" theory, which argues that the self-management principle implies a fallacy assumption that people behave rationally. There are many

[104] Id., at 139.

[105] GDPR, article 82 – 83.

[106] Shyy, *supra* note 38, at 160.

factors that influence people’s choices in a manner that can be unavoidable. Thus, the theory proposes the usage of techniques that nudge people towards their welfare without omitting any options.[107] Their argument is liberalism in the sense that it grants the individual access to all available options, and it is paternalistic in the sense of assigning a planner the job of "self-consciously attempting to move people in welfare-promoting directions."[108] In this part, I demonstrate the irrationality of people's actions, the inevitability of intervention, and the role of nudges in promoting the freedom of choice.

1. **Irrationality:**

The self-management principle claims that individuals act and choose what is in their best interests. However, based on phycological experiments, Thaler and Sunstein argue that people's decisions and choices are irrational.[109] They refer to dozens of experiments and researches that prove that people's choices are influenced by external factors that shape their preferences. Ironically, people reflect on some nudges like: 1. Unrealistic optimism or overconfidence 2. The fear from losses than gains. 3. Status quo bias.[110] Moreover, framing also has a considerable effect on the individual, which can alter their decisions.[111] The wording of options or information can shift an individual's actions surprisingly. Meanwhile, on many occasions, they lack sufficient time and/or information to think and analyze the available choices. In other situations, they decide automatically without paying full attention to the details.[112] Phycologists notice that individuals' decisions are dynamically inconsistent.[113] Therefore, the outcome might not be the best for their own welfare.

Individuals depend on tools and other people to help them to make some decisions. They write lists to remember what to buy. They rely on alarms to wake them up. When they face complicated choices or they do not have the time to think about them, they depend on what companies chose for them, which is known as the *default* option. Research shows

[107] Sunstein & Thaler, *supra* note 4.

[108] Cass R. Sunstein & Richard H. Thaler, Libertarian Paternalism Is Not an Oxymoron, 70 U. CHI. L. REV. 1159 (2003), at 1162.

[109] *See* Richard H. Thaler, Cass R. Sunstein, Nudge_ Improving Decisions About Health, Wealth, and Happiness (2008).

[110] Id., at 33-35.

[111] Id., at 37.

[112] Id., at 43.

[113] Id.

that individuals would highly likely stick with the *default* option that has been chosen by other parties, like what we do when we install a new software program.[114] Individuals do trust others who could take advantage of such behavior. Furthermore, experiments proved that people follow the steps of others even if they know that their judgments are wrong.[115] For example, one will choose A if she chose privately, but when she knows that the group chose B, she will probably choose B also, even if B is the wrong answer. Moreover, individuals care about the group's opinion, which can make them behave differently because they fallacy think that they are paying attention to him/her and fear from others' disapproval, which is known as the *spotlight effect*.[116] The power of those influences makes people's decisions unpredictable.[117]

2. **The Inevitability of Influencing People's Choices:**

Many scholars argue that a true libertarian will not advocate any paternalistic intervention in individual's choices. They refuse any kind of influence because it undermines the individual autonomy who should have the liberty to act freely "regardless of whether individuals use their liberty wisely."[118] Gregory Mitchell argues that a true libertarian does believe that "no social goal can justify forcing an innocent individual to be a resource for others."[119] Thaler and Sunstein should work on improving people's freedom of choice instead of participating in the manipulation.[120] Therefore, governments should refrain from

[114] Id., at 8.

[115] Id., at 58-59. (People were asked, "Which one of the following do you feel is the most important problem facing our country today?" Five alternatives were offered: economic recession, educational facilities, subversive activities, mental health, and crime and corruption. Asked privately, a mere 12 percent chose subversive activities. But when exposed to an apparent group consensus unanimously selecting that option, 48 percent of people made the same choice!).

[116] Id., at 57.

[117] Id., at 62. (In an experiment, they created eight worlds who will listen to list of songs. Each world divided to two groups. Each group would have the ability to hear all songs but only one group would have the ability to know how many times each song was downloaded. In all eight worlds, individuals were far more likely to download songs that had been previously downloaded in significant numbers, and far less likely to download songs that had not been as popular. Most strikingly, the success of songs was quite unpredictable, and the songs that did well or poorly in the control group, where people did not see other people's judgments, could perform very differently in the "social influence worlds. The identical song could be a hit or a failure simply because other people, at the start, were seen to choose to have downloaded it or not.).

[118] Gregory Mitchell, Libertarian Paternalism Is an Oxymoron, 99 NW. U. L. REV. 1245 (2005), at 1260.

[119] Id. at 1272.

[120] Id. at 1255.

any try to practice paternalistic influences on individuals because such tries conflict with the individual right to self-management.

However, this critique is based on the assumption of the possibility of avoiding the influences factors. It is almost impossible for individuals to avoid the influences that shape their preferences and choices.[121] As illustrated previously, individuals' choices are affected by psychological and social influences that drive them towards a specific direction. On many occasions, corporates and advertisers have to take action that will alter consumers' behavior. They have to choose the default option for consumers; otherwise, people would feel lost or even abandon their services. They take advantage of the understanding of human behavior and try to influence them to boost their sales. For example, some advertisements emphasize that "most people use" a specific product because they know that people respond to such messages. Moreover, framing is inevitable. There is almost no neutral way to display choices. Corporates and governments frame the context in a way that can change people's answers. For example, shaping the options as a loss or a gain could significantly change the results.[122] Therefore, influencing people's decisions is inevitable.

3. **Nudges:**

Since people do not act in their own best interest and choices influences are inevitable, nudging them to act wisely seems to be the right path in order to make their lives better. While corporates and governments are taking advantage of people's weaknesses to achieve commercial and political objectives, libertarian paternalism aims to enhance people's lives. Thaler and Sunstein argue that the freedom of choice can be promoted by using techniques that architect choices to change "people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[123] The objective of the planner, the one who will architect the options, is to promote individual welfare. One of the significant examples of using libertarian paternalistic nudges is the usage of health warnings on cigarette packages. According to the WHO, those pictures and warnings are associated with increased motivation to quit smoking.[124] Nudges differ from mandates; the

[121] See Sunstein & Thaler, *supra* note 108.

[122] Cass R. Sunstein, How Law Constructs Preferences, 86 GEO. L.J. 2637 (1998), at 2647.

[123] Thaler & Sunstein, *supra* note 109, at 6.

[124] https://www.who.int/bulletin/volumes/87/8/09-069575/en/

latter motivates individuals by imposing some burden on them like taxes and fines or giving them some advantages like subsidies. Unlike mandates, nudges impose no burden on people with almost no cost, which makes it a good policy for policymakers and more welcomed by individuals.[125]

Recently, many governments started to use nudges to implement certain policies. In the UK, the government created the Behavioral Insights Team, also known as the Nudge Unit, which uses behavioral insights to improve public policies.[126] While the US, Australia, Canada, Sweden, Netherlands, and Germany also created their own teams, other countries like India, Indonesia, Peru, and Singapore are working on establishing their behavioral insights teams.[127] Some international organizations like the World Bank, UN agencies, OECD, and EU formed similar units to support their programs. The World Bank also issued a full report on behavioral informed tools which focuses on nudging.[128] Those teams are working on improving many policies such as poverty, obesity, gender equality, crime reduction, and energy consumption. For instance, they write the number of calories and reorganize the food order in menus which helps people to choose healthier food. They architect the choices in a manner that can promote individuals' lives.

Nudges have proved its effectiveness in many fields when it is used correctly. People do not respond positively to all nudges. Choices have to be architected in certain ways that consider what people like and what they do not. Informing people has its positive effects on people. An experiment revealed that people respond to positive wording than negative ones.[129] In Minnesota, for example, using legal threats did not improve the number of taxpayers, but when officials inform them about the high compliance level, people tend to be more compliant.[130] In fighting littering on Texas highways, releasing a well-funded campaign did not have a big impact on citizens' behavior, but when public officials used a

[125] Cass R. Sunstein, Do People Like Nudges, 68 ADMIN. L. REV. 177 (2016), at 200.

[126] David Halper, Inside the Nudge Unit: How small changes can make a big difference (2015) (showing how the Behavioral Insights Team created solutions in tax, healthcare, crime reduction, and spurred economic growth.).

[127] Zeina Afif, "Nudge units" – where they came from and what they can do, https://blogs.worldbank.org/developmenttalk/nudge-units-where-they-came-and-what-they-can-do

[128] World Band, Mind, Society, and Behavior (2015), https://www.worldbank.org/content/dam/Worldbank/Publications/WDR/WDR%202015/WDR-2015-Full-Report.pdf.

[129] Thaler & Sunstein, *supra* note 109, at 66.

[130] Id., at 66.

creative slogan "Don't Mess with Texas" in another campaign, there was a decrease in litter by 29%.[131] Moreover, people do not support nudges that do not align with their values or beliefs. They also reject nudges that have illegitimate or illicit goals.[132] Similar results can be seen in different countries that have different cultures and values.[133]

On the other hand, nudges do not offer an ultimate solution for every problem. Nudges help to improve people's decisions, but, in some instances, they have to be associated with other social and legal tools to have better results. Alberto R. Salazar V. argues that nudges have a short-term impact on fighting obesity.[134] People need more than nudges to change their attitudes and values. Moreover, many parties, motivated by commercial and political incentives, would undermine the libertarian paternalism' nudges by fighting back with all the power they have. They would spend more money on ads and nudges that push consumers to buy their products because their interests contradict with people's welfare in many situations. It is problematic to ensure their obedience to healthy nudges. For example, unhealthy foods' ads can undermine the effects of reorganizing food menus. Therefore, libertarian paternalism's nudges should be supplemented by legal rules that forbid or reduce opposite nudges.

4. The Planner’s Critiques:

Many scholars propose the following questions: what are the limitations of using nudges? How can we assure that the planner would not use those powers to manipulate and extend the usage of nudges in other fields for other purposes? Who is the planner? And could a planner do better than the individual? Gregory Mitchell argues that "it is impossible by definition for a third party to make judgments about another individual's utility."[135] Even if the individual fails to make a good choice, there is no evidence that another party would succeed to do better. Moreover, some concerns are derived from the mistrust of the planner's identity and his/her ability.[136] People do not trust public officials; they are suspicious about their intentions and plans because government image is usually associated

[131] Id., at 60. (In its first six years, there was a 72 percent reduction in visible roadside litter.)
[132] Sunstein, supra note 125, at 185.
[133] Id., at 201-205 (mentioning surveys from Sweden and USA.)
[134] See Alberto R. Salazar V., Libertarian Paternalism and the Dangers of Nudging Consumers, 23 K.L.J. 51 (2012).
[135] Mitchell, *supra* note 118, at 1267.
[136] Sunstein & Thaler, *supra* note 108, at 1200.

with power, control, coercion, and political agenda. Conversely, they mostly welcome a planner from private institutions.[137] Furthermore, many scholars accuse libertarian paternalism of being manipulative.[138] Authorizing the government to affect people's decisions is an invitation to manipulate the people. Choices have to be presented to the people equally and supplemented by sufficient information to construct better decisions. In contrast, architect the choices in a manner that makes individuals choose a specific choice is a manipulation, even if it is a better choice, because the planner "intentionally bypass or circumvent someone's rational capacities."[139]

All previous critiques revolve around the planner. There is mistrust in the planner's identity and role. In fact, these worries are logical. Nudges are used to redistribute the power between private companies and governments. This power can be abused by governments as much as corporates do. In non-democratic states, the government can misuse nudges to achieve its political goals. However, such critiques do not mean that nudges should not be used. Conversely, those critiques enlighten the path that nudges should be used carefully and under levels of scrutiny. A "nudge unit" should work under the parliament and judiciary supervision and according to a code of ethics. People's representatives are more trustworthy to regulate the planner's role. Legislators should specify the scope of the planner's work by identifying the problems that they can deal with and the tools that they can use, and the ethics they should stick to. Meanwhile, judicial supervision over the planner work is also a guarantee for the protection of people's rights. Courts can terminate the manipulative nudges. Finally, nudges should be supplemented by media campaigns that aim to raise users' awareness because being aware of the problem would improve individuals' ability to choose. For example, an aware user can effectively protect his/her personal data. He/she is more likely to respond positively to privacy nudges.

On the other hand, the planner could not force people to choose a specific choice; conversely, individuals will always have the upper hand to accept or reject the nudges. Even though libertarian paternalism reorganizes the choices hoping to move people

[137] Thaler & Sunstein, *supra* note 109, at 10.

[138] *See* Jason Hanna, Libertarian Paternalism, Manipulation, and the Shaping of Preferences, 41(4), Social Theory and Practice: An International and Interdisciplinary Journal of Social Philosophy, 618 (OCT 2015); Mitchell, *supra* note 118.

[139] Id., at 625.

towards a specific direction, it does not exclude any choices. This characteristic leaves room for individuals to reject nudges and choose whatever they want. Moreover, experiments show that people reject nudges that have illegitimate ends or contradict their personal values and standards.[140] They support the nudges that they agree with their purposes. In the meantime, many people could take a very strong position against certain nudges if they felt that they aim to control or heavily intervene in their lives. "[P]eople do not like being controlled or coerced, and if they think that their options have been truncated, they might do whatever they can to take their own path."[141] Thus, if the government uses nudges for other purposes rather than people's welfare, people would reject them.

Finally, because choices' influencing is inevitable, a planner that aims to provide better choices architecture is a must. It is unlogic to leave the people as prey for corporates who manipulate them to gain commercial benefits. The nudges should be used to stop or mitigate the harms that occur from excessive ads that urge them to eat unhealthy food and smoke cigarettes. Furthermore, the opponents assume that there is "neutral" choice architecture.[142] However, this assumption is incorrect. As I argued, people are always influenced by the context in which they have to make a decision. Even if the wording can be written in neutral language, there are always external or internal factors that affect an individual's decision.

[140] Sunstein, *supra* note 125, at 198.

[141] Id. at 222.

[142] Hanna, *supra* note 138, at 640.

V. Nudging Users Towards Online Privacy

Libertarian paternalism can be a solution for what current policies and regulations could not resolve. Privacy policies are hard and long to read, which impedes users' abilities and willingness to read them. In addition, the GDPR and the Egyptian law for personal data protection No. 151 of 2020 chose to empower users with a bundle of rights. However, empowering users is not effective because users are not aware of or capable of using those rights. These legal tools overlooked the complexity of human beings and how they interact with the internet. Therefore, the libertarian paternalism theory can fill in the gap. Nudges can be a complementary solution that is based on understanding human behavior in order to alter users' decisions towards more privacy.

In this chapter, I analyze the online privacy problem in light of the libertarian paternalism theory. In the first part, I demonstrate the irrational behavior of internet users regarding their privacy which is known as the "privacy paradox,"[143] and the causes behind this phenomenon. Users claim that they have concerns about their online privacy and are aware of their rights, but they act conversely. Due to external influences, they recklessly disclose much personal information and give permission for a huge number of tech companies to collect and transfer their personal data throughout their daily online activities. In the second part, I illustrate the advantages of using nudges and engage with the planner critique. Finally, I present a number of nudges examples that can be used to improve online privacy.

A. Data Subjects' Irrationality:

Data collectors and holders take refuge in self-management. Tech companies simply argue that people are free to choose whatever they want. Users agree on their terms and conditions, which grants them the right to collect the data and share it with third parties. They also willingly disclose their personal data and share their photos and stories with others. No one coerces them to do any of those acts. On the other hand, the government should refrain from any intervention that would undermine people's freedom of choice. It ought to protect their freedom. However, this argument is based on three related assumptions. It assumes that users: (1) act rationally; (2) are truly free from any kind of

[143] Sheng Yin Soh, Privacy Nudges: An Alternative Regulatory Mechanism to Informed Consent for Online Data Protection Behaviour, 5 EUR. DATA PROT. L. REV. 65 (2019).

influence; (3) choose what is in their best interest. In my opinion, these assumptions are false. In this part, I argue that users act irrationally over the internet regarding their privacy because they are affected by inevitable social and commercial influences.

People seem to act in the opposite direction of their true desires. As Sunstein and Thaler argue, people act irrationally and choose what is not in their best interest. They want to be healthy, but they smoke cigarettes and eat unhealthy food, although their bad consequences on health. They care about their online privacy,[144] but they explicitly or implicitly reveal a massive amount of data about themselves. As previously demonstrated in chapter three, the erosion of online privacy has enormous harm on individuals and society. Many users know the risks of their online activities, but they do nothing to avoid the causes. Users harm themselves by their online actions. Accordingly, the question that arises is: why do people act irrationally and choose the worst in their interest?

Even though it appears that users voluntarily agree to disclose and share their personal information with others, they are influenced by social and technical influences that limit their freedom of choice. Online platforms enable easier methods of data disclosure than their offline counterparts. Users easily share their photos and comment on posts without the necessary attention that they give when they are dealing with strangers in real life. Moreover, people have to accept the terms offered by tech companies in order to benefit from their services. In the internet world, an individual cannot live without the services of Google and Facebook; he/she is compelled to accept their terms and give them permission to access and collect data from personal devices.

In order to make a good decision, an autonomous user has to be well informed and has the ability to understand and analyze the choices at hand. Users should receive sufficient information about the collected data, and they should have a choice about the usage of that information, which is known as "notice and choice."[145] However, studies reveal that users do not have the ability to make such informed and rational choices.[146] Scholars like Richard

[144] Share of internet users who are more concerned about their online privacy compared to a year ago as of February 2019, by country, https://www.statista.com/statistics/373322/global-opinion-concern-online-privacy/ (statistics show that more than 50% of users around the world are worrying about their privacy.)

[145] Howard Beales II. & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information, 75 U. CHI. L. REV. 109 (2008), at 112.

[146] Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880 (2013), at 1883.

Warner and Robert Sloan argue that informed consent is impossible due to the complexity of data collection systems.[147] People's irrationality happens due to multiple reasons. First, in order to have a rational choice, a user has to read the terms and privacy policy to be informed about the data collected. Studies show that only a few users read privacy policies.[148] Privacy policies are complex; it is overwhelming to read and understand them.

Privacy policies are usually long and complex, which makes them time-consuming to read each privacy policy in every website and application a user uses or visits in his/her daily activities. A research found that each user needs 40 minutes per day to read each privacy policy which is more than the time he/she spend for shopping, playing games, and dealing with spams combined.[149] Meanwhile, if every American user read all privacy policies at websites they visited in one year, it would cost the economy 781 billion dollars in lost productivity.[150] Nonetheless, a privacy policy should not be short and easy because it will not be informative enough to enable users to make an informed decision because privacy is a complicated issue. People need more information to understand: what are the types of collected data? How would it be used, secured, and processed? What are the limitations of transferring those data to third parties? What are their rights regarding their collected data? Therefore, a long policy is needed to demonstrate such issues effectively.

Moreover, data privacy usually intersects with technical issues that people could not understand. As Prof. Helen Nissenbaum argues that it is "so complicated that probably only a handful of deep experts would be able to piece together a full account."[151] Most people lack the technical background to fully understand the policy. Privacy policies contain much complex and legal jargon. Many people are not aware of the legal or technical definition of many words that are being used in privacy policies. Studies show that people have false beliefs regarding their online privacy, which reveals that people do not fully understand

[147] Shyy, *supra* note 38. (mentioning Richard Warner & Robert Sloan, Beyond Notice and Choice. Privacy, Norms, and Consent, 14 J. HIGH TECH. L. 370 (2013).)

[148] Solove, *supra* note 146, at 1884. (mentioning a study that shows that only 20% of users read privacy policies most of the time); Beales & Muris, *supra* note 145, at 113.

[149] *See* Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 ISJLP 543 (2008), at 563.

[150] *Id*., at 564.

[151] Helen Nissenbaum, A Contextual Approach to Privacy Online, 140 DEDALUS THE JOURNAL OF THE AMERICAN ACADEMY OF ARTS & SCIENCES 32 (2011), at 35.

privacy policies.[152] Meanwhile, tech companies take advantage of this position by getting users' approval on the collection and distribution of data by writing long, broad, and complex privacy policies that are hard to be read or understood by most users.[153] A German court found that a user's consent on Facebook's privacy policy is invalid because it hides important privacy settings in its policy.[154] Meanwhile, trying to demonstrate each detail in privacy leads to an opposite effect. Detailed information is needed to more transparency, "but too much information leads to a lack of transparency," which Prof. Helen Nissenbaum called the "transparency paradox."[155]

Furthermore, the way the privacy decision is designed leads to severe troubles to reach rational choices. A user needs to decide which data will be revealed before he/she visits the website. He/she needs to assess the potential harms from disclosing some information when the data is initially collected, which is very hard to predict.[156] For example, the harm from data *aggregation* and *transferring* is unpredictable. A user might not know that a small piece of data can be combined with other small pieces revealed on other websites at different times to reveal sensitive information. Technology develops constantly; a piece of data could not be combined with other data to reveal other types of information now, but a method can be discovered in the future to do so. Therefore, it is extremely difficult to assess privacy's harms while making the decision.

On the other hand, tech companies use multiple strategies that nudge users to abandon their privacy. Social platforms exploit users' trust to share more information.[157] Most companies use the "opt-out" strategy, which means that people are automatically enrolled in accepting the data collection. It would need action from the user to opt-out, which is not the common behavior of humans.[158] They also use the "default" option in their favor. They adjust the default option in a manner that gives them the authority to collect the data they

[152] Solove, *supra* note 146, at 1886. (They correctly answered only 30% of the questions regarding their online privacy.)
[153] See Tsesis, *supra* note 9.
[154] Facebook broke German privacy laws, court rules, BBC, https://www.bbc.com/news/technology-43035968
[155] Nissenbaum, *supra* note 151.
[156] Solove, *supra* note 146, at 1891.
[157] Shyy, *supra* note 38, at 146.
[158] Solove, *supra* note 146, at 1884.

need. They know that people rarely change the default privacy settings.[159] In addition, they architect the choices carefully. While they use positive language when they ask for permission for collecting data, such as "enhancing your experience," they use negative words when one needs to opt out, like "this action might affect the service." This method frames people's thinking about the action they would take and implicitly nudge them towards a specific direction.

Moreover, Tech companies intentionally intervene in shaping people's preferences, and beliefs which undermine privacy self-management. An autonomous individual needs to be free from such intervention and monitoring. Many scholars note that online platforms "can nudge users to form beliefs and preferences, follow behaviors, and increase the probability of outcomes with ever-finer precision."[160] Personalization allows tech companies to control what users can see and what they cannot. Such power is used o manipulate people and shape their preferences in order to achieve commercial and political goals, as I illustrated earlier in chapter two. Furthermore, they exploit the human weaknesses regarding their social needs to communicate with others. They architect their programs and software to enhance users to engage with other users and share more information, pictures, and stories to make new friends or profound their relation with current ones. In conclusion, users are irrational regarding their online privacy because they are influenced by multiple factors and parties that affect their freedom of choice.

On the other hand, the assumption that people choose what is in their best interest is also false. Libertarians argue that individuals choose wisely, and the state should not intervene unless there is substantial harm to others that justifies the intervention. However, people's online choices regarding their privacy are not only in their worst interest, but also their actions lead to substantial harm for individuals and societies. As illustrated in chapter three, privacy erosion causes damage to individuals' reputations, dignity, and emotions. It increases the possibility of committing many wrongful acts like fraud, impersonations, blackmailing, and defamation. In addition, it leads to the spread of false news and polarization, which jeopardizes democracy and creativity. Even though some scholars claim that the benefit of data flow outweighs the harms of privacy harms. They emphasize

[159] Id.

[160] Grafanaki, *supra* note 84, at 6.

the great importance of data collection and dissemination for social and scientific purposes.[161] Even though I disagree with this opinion, I am not arguing for the prevention of data collection or distribution. Instead, I argue that online privacy has to be regulated in order to mitigate the harm by nudging users towards their welfare. Therefore, an intervention is legitimate and required.

B. Online Nudges:

Nudges offer a balanced solution that can help to mitigate the privacy harms. First, they would not coerce people to choose something. No choices will be omitted; instead, choices would be reorganized and architected to promote privacy. Users would be free to disclose whatever they want, but they would be warned first about the risks. Meanwhile, users would not be left alone in the face of greedy data collectors. Moreover, nudges would help individuals make better choices and avoid harm. It aims to architect the choices in a manner that help user to understand the complex choices and aware them with simple tools about the risks of personal data disclosure.

Behavioral economics scientists prove that people tend to use the "fast-thinking system" in their routines activities which are repeated on a daily basis.[162] In online activities, users use their intuitive, instinctive, and rapid way of making decisions because most of them use the internet daily for hours. They do not spend too much time in deciding which privacy settings they will choose. Thus, privacy settings should be simple and easy to understand. People respond to an image more than a long text[163]. Nudges include, for example, using the most privacy-friendly choices as a default, simplifying privacy settings by using images, characters, and emojis, informing users about the real audience for their posts, and delaying for seconds before posting personal stories.[164] Those tools can overcome privacy complexity by introducing the information in easy ways that most users can understand. They increase the effectiveness of notices, especially when they are provided immediately before taking the decision because it is the perfect moment to make

[161] See Swire, *supra* note 45.

[162] Shara Monteleone, Addressing the Failure of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation, 43 Syracuse J. INT'l L. & COM. 69 (2015), at 105.

[163] Id., at 108.

[164] See Yang Wang, Pedro Giovanni Leon, Xiaoxuan Chen & Saranga Komanduri, From Facebook Regrets to Facebook Privacy Nudges, 74 OHIO St. L.J. 1307 (2013); Soh, *supra* note 143.

them rethink about their upcoming decisions.[165] Therefore, libertarian paternalistic measures would help to promote privacy, users' welfare, and privacy self-management.

Nudges is also useful for the data industry. Conversely to the GDPR, nudges are less burdensome on small companies. New entrepreneurs would not need to spend much money to implement.[166] Even though promotion of privacy would cost tech companies the loss of some data, they would gain the trust of users, which would lead to more disclosure of *necessary data* for the business.[167] An enhancing privacy architecture assures consumers that the service provider is caring about their data and would not use them wrongfully. Therefore, libertarian paternalism offers a robust and balanced solution that would help to promote online privacy and the data industry while building and protecting actual freedom of choice.

Choice architecture, however, has to be designed carefully to ensure its effectiveness. Thaler and Sunstein define nudges as "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[168] The first step to implement nudges is to understand the human's way of thinking and how individuals react to different nudges in order to architect the choices in a manner that can alter their decisions. Economic behavior literature reveals several reasons for Individuals' biases like status quo and spotlight effect, which I illustrated previously in chapter four.[169] Those reasons should be taken into consideration to design a successful nudge.

Moreover, a good nudge expects users' errors. People err in using equipment or making a decision. For example, a study found that 82% of critical incidents are caused by human errors.[170] The planner should expect such errors and try to be "as forgiving as possible."[171] In addition, a well-designed nudge has to transform complex and long choices into simple ones by helping users to map the choices easily. As Thaler and Sunstein mentioned, it can

[165] Cinthia Obladen de Almendra Freitas & Giovanna Michelato Almada, How Can Nudging Solve Some of the Internet Data Privacy Issues, 10 DIREITO e Desenvolvimento 7 (2019), at 14.

[166] Shyy, *supra* note 38, at 164.

[167] Shara Monteleone, Addressing the Failure of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation, 43 Syracuse J. INT'l L. & COM. 69 (2015), at 115.

[168] Thaler & Sunstein, *supra* note 109, at 6.

[169] See id.; Monteleone, *supra* note 166, at 97.

[170] Thaler & Sunstein, *supra* note 109, at 89.

[171] Id. at 87.

be done "by transforming numerical information into units that translate more readily into actual use."[172] One example can be showing users actual information like current location or device information that would be collected if they agree on the website's terms.

However, the planner's critiques is one of the main critiques of libertarian paternalism that should be taken seriously in dealing with online privacy. The planner's role should be collaborative work. In other words, it should not be assigned to one person or entity. First, an international agreement is needed to regulate the data market. Data market values billions of dollars, and citizens' data is vital to the national security of states. Countries have to agree on the rules that regulate that market. In such an agreement, there should be rules that aim to decrease the privacy risks and regulating the usage of privacy nudges. Such international standards would prevent the misuse of nudges. Moreover, the planner job should be assigned to a board of stakeholders' representatives like governments and giant tech with a majority of experts in sociology and technology that have the expertise, knowledge, and awareness of the negative effects of privacy violations. In 2019, Facebook started a plan to establish an "Oversight Board," which should be an independent entity that will have the power to review Facebook's decisions regarding the removal of individuals' posts.[173] Even though it would be hard to imagine a global collaboration to deal with online privacy, a similar entity can be established to put an ethical code and alternative techniques that would promote privacy. Such an entity would provide room for more discussions between stakeholders in order to respond to their inquiries and concerns. Moreover, online privacy is a complex problem that constantly evolves with the development of technology which requires a similar development in tools that aim to promote privacy. In addition, a respectful, independent entity would gain people's trust, which would reflect on their response to nudges. Thus, an independent entity is needed to play the planner role. Until such an entity exists, a governmental entity can play this role under the scrutiny of the parliament in order to monitor its performance and prevent manipulation.

[172] Id., at 92.

[173] Brent Harris, Establishing Structure and Governance for an Independent Oversight Board, https://about.fb.com/news/2019/09/oversight-board-structure/

On the other hand, nudges have to be complemented with other legal tools that would help to regulate online privacy. A nudge helps improving people's decisions, but it has to be associated with other social and legal tools to ensure its effectiveness. Implementing nudges to online privacy may not be welcomed by any data collectors because such a policy would impede their access to various kinds of data. It is not expected to apply such techniques through a self-regulating system. It has to be implemented by legal regulations. Law is essential to enforce tech companies to adopt the proposed techniques, as done in implementing nudges in the smoking issue. Meanwhile, using nudges to promote privacy requires the prohibition of nudges that aim to the opposite. Privacy nudges could be jeopardized by counter influences motivated by commercial entities.

Moreover, governmental institutions have to work to ensure the compliance of tech companies with their privacy policies because some studies have proven that many corporates do not comply with their own policies.[174] Finally, the law is required to regulate the personal data, which their collection is necessary for the service. Privacy nudges aim to minimize the disclosure of personal data, but online services are based on users' data. There will always be necessary data that is collected, processed, and transferred, which should be regulated by coercive regulatory tools.

C. Nudges Examples:

1. Privacy by Default (Status Quo):

Privacy-enhancing features should be incorporated in the design of websites and programs which is known as "privacy by design" or "privacy by default." It is "a systematic approach to designing any technology that embeds privacy into the underlying specifications or architecture."[175] Many scholars pointed out the strong impact of the default settings on online privacy.[176] If preventing websites and applications from access to location, contacts, and the gallery is the default, privacy will be less violated. Public and private entities take advantage of the immense power of default settings. When users face multiple complex choices, they depend on others to decide which option they will choose. For example, people are more likely to keep the checked box "regular" or "custom" option

[174] Monteleone, *supra* note 166, at 116-117.

[175] Ira S. Rubinstein, Regulating Privacy by Design, 26 BERKELEY TECH. L.J. 1409 (2011).

[176] Soh, *supra* note 143, at 72.

when they install new software.[177] Using privacy-enhancing as a default is powerful in promoting privacy because people tend to keep their status quo.[178] In other words, they rarely change the default settings. However, the take-it or leave-it strategy could jeopardize the default nudge.[179] If the website requires the changing of "privacy enhancing" default to another choice to benefit from its services, users would be compelled to change it because most users could not bear such a burden. Therefore, this strategy should be abandoned.

Privacy by default has been implemented recently. The GDPR admits the importance of privacy by design in promoting privacy. Under article 25 of the GDPR, data collectors are obliged to collect "by default, only personal data which are necessary for each specific purpose of the processing are processed."[180] They have to ensure, by default, that those data "are not made accessible without the individual's intervention to an indefinite number of natural persons."[181] In another occasion, Mozilla prevented, by default, third parties' cookies to Firefox; in 2013, they updated the website browser by allowing only cookies from websites that were visited.[182] In other words, the user has to change this setting by themselves to allow third parties' cookies. The new update led to a positive improvement in privacy because users stick with the default option.[183] Therefore, privacy by default can lead to a significant improvement to online privacy without imposing any duties or costs on users, governments, or tech companies.

2. **Profile Nudge:**

One of the biggest users' regrets on social media is that they do not realize the real audience to their posts until they publish. People share their stories and pictures on social media platforms with false expectations about who will see their posts.[184] They think that only some friends in their minds would see it. However, they realize after a while that there is an unintended audience who definitely does not want to share their thoughts with, which leads to many regrets.[185]

[177] Thaler & Sunstein, *supra* note 109, at 83 - 87.
[178] Id.
[179] Soh, *supra* note 143, at 72.
[180] GDPR, Article 25.
[181] Id.
[182] Freitas & Almada, *supra* note 165, at 14.
[183] Id.
[184] Wang, *supra* note 164, at 1320.
[185] Id.

One research developed the "profile picture nudge" that deals with this problem.[186] It works by displaying five random profile pictures of the audience who can see the post before publishing it. The nudge aims to notify the user of the potential audience in order to think before posting. The nudge also informs the user of his/her privacy settings by stating clearly which categories can see the post, i.e., friends, or friends of friends. The experiment showed that the nudge made users change their behavior by being more cautious about their posts, changing their privacy settings, and removing some 'friends.'[187] This nudge allows users to assess the situation based on real and simple facts that helps them to understand the risks and the choices beforehand. It also provides the information just before making the decision, which is vital in forming the final decision. Therefore, this nudge succeeded in improving privacy choices.

3. **Timer Nudge:**

A research found that users regret sharing many posts about their emotional, political, and religious opinions. The research found that a few seconds delay before a post is actually published is helpful in encouraging people to avoid unnecessary data disclosure. Researchers designed the "timer nudge" that creates a ten-second gap before the actual post. A message will appear while typing a post stating, "you will have 10 seconds to cancel after you post the update."[188] They used a yellow background to be recognized as a warning. The user will have ten seconds after hitting the post button to think with an available option to cancel or edit the post before the publishment. They also provided the users with an option to override the nudge by clicking "post now."[189] The nudge aims to give the users the time to rethink and alter their decision if they want to. The experiment showed that while some users rephrased their posts, others preferred to cancel the post.[190] These findings are supported by other scholars who emphasize the importance of the timing factor in promoting privacy.[191]

[186] Id. at 1321.

[187] Id. at 1322.

[188] Id. at 1331.

[189] Id.

[190] Id.

[191] Soh, *supra* note 143, at 72. (citing Serge Egelman et al, 'Timing is everything?: the effects of timing and placement of online privacy indicators' (Proceedings of the SIGCHI Conference on human factors in computing systems, Boston, April 2009) 319-328.).

4. **Content Feedback:**
Sunstein advises that providing feedback to the consumers is the best method to improve their behavior.[192] People are nudged when the system tells them about their mistakes and achievements. Meanwhile, social media facilitates the sharing of thoughts with large number of people which can be regrettable in many occasions, especially when they post about controversial topics. Researchers created the "sentiment nudge" that works on giving the user feedback on the content of the post before posting it.[193] The nudge is composed of timer delay, yellow background, and a sentence that reflects the content of the post. For example, if a user writes "I am angry," the system will warn him/her that "other people may perceive your post as negative."[194] Within few seconds, the user could edit or cancel the post.[195] The main objective of this nudge is to aware users of how other people may perceive their posts.[196] When they realize that their posts can be misunderstood, they could change them, aiming to prevent unwanted disclosure.

Even though the experiment's findings were not positive, this nudge can be developed to be more effective. Some participants dislike the nudge because it lacks the knowledge of context that motivates them to write the post and because it is judgmental;[197] others ignored the nudge.[198] However, the nudge might be effective with teenagers because they lack the needed experience and pay more attention to how they look in their peers' eyes. In addition, the software can be changed to be simpler, like using characters or emojis that reflect the wording of the post in order to be more friendly. Finally, nudges can be developed to pop up only when the post could lead to a disclosure of sensitive information or when it might lead to emotional harm.

5. **Simple, Visible, and Salience:**
One of the influences that could affect people's behavior is making certain things *visible and salient*.[199] The salience of certain features like prices, sizes, or incentives can nudge

[192] Thaler & Sunstein, *supra* note 109, at 90.
[193] Wang, *supra* note 164, at 1322.
[194] Id.
[195] Id.
[196] Id. at 1331.
[197] Id.
[198] Id., at 1333.
[199] Monteleone, *supra* note 166, at 105.

consumers to behave in a predictable way.[200] It also can affect people if it is provided in a salient moment or situation. The information can be salient by using different colors, capitalizing, and increasing the font size of a specific word. Users have to be informed with actual data collected from them instead of giving vague notices. If the user realizes the amount of personal data collected, he/she would think twice before granting the permission of collection. So, instead of asking for users' consent to collect their IP, location, and device details, the notice should provide them with a message that contains their actual IP, location, and other collected data. The system should make the message visible and salient.

It could also be done by making certain information more visible. For example, increasing the prices of electricity will affect individuals' consumption if the government made the increase salient, but if the consumers were able to receive notifications of the actual cost, many of them would probably reduce their consumption.[201] However, there is one condition to succeed in nudging users towards privacy: "do not, by any means, let them know that their current actions are better than the social norm."[202] When people know that their behavior is above-average, they tend to change their behavior in the opposite direction, which is known as the "boomerang effect."[203] Therefore, providing too much information might lead to unwanted behavior.

The solution is to give them a simple indication that their behavior is socially acceptable or not. One of the effective ways is the usage of nonverbal signals in describing the user's behavior.[204] Regarding online privacy, a nudge can be designed to translate complex choices into a simple emoticon. Using emoticons proved its effectiveness in reducing energy consumption in California.[205] A similar approach can be applied to online privacy; the most enhancing privacy choice would be represented by a happy emoticon, whereas the worst would be represented by a sad or angry emoticon. Moreover, a nudge can work as a data meter that can monitor the amount of data collected by different websites and apps. It would raise an emoticon that alerts users when the data collector breaks a certain threshold. Such nudges would overcome the boomerang effect.

[200] Id.
[201] Thaler & Sunstein, *supra* note 109, at 99.
[202] Id., at 68.
[203] Id.
[204] Id.
[205] Id.

On the other hand, using interactive characters is problematic. Nudges can be simplified by using less text and more interaction which is known as "visceral notices."[206] It successfully influences the user's fast thinking by showing them instead of telling them.[207] Designing an interactive character that interacts with the user while using the internet can affect the user's behavior regarding the data disclosure. Shara Monteleone argues that this type of nudges is effective in "reducing data disclosure without creating privacy concerns."[208] In contrast, another study showed that using anthropomorphic characters nudged people to reveal more personal data due to the increasing levels of trust.[209] Thus, more researches have to be conducted in order to redesign these types of nudges to ensure their effectiveness in promoting privacy.

[206] Monteleone, *supra* note 166, at 110.

[207] Id., at 111.

[208] Id., at 112.

[209] Id.

VI. Conclusion

Indeed, data is the most valuable resource on the planet because it is essential to the stability of the internet. While Tech companies collect massive amounts of data in order to provide and develop their services, billions of users depend on the internet, among other things, to conduct researches, buy products, play games, communicate with friends and family members, and spend their leisure time. However, such practices are associated with privacy violations. Advanced algorithms are able to collect and analyze a vast amount of data. They track each activity for each user on the internet. They are able to reveal sensitive information by combining small pieces of data. Such information can be misused by tech companies and governments to influence users to achieve commercial and political objectives.

Although defining privacy is problematic because it intersects with many other rights, privacy can be defined by identifying the harms that happen to individuals and society. Online privacy harms occur while collecting, processing, and disseminating data. Throughout these stages, people suffer from various types of harm like interrogation, surveillance, identity theft, fraud, and reputational and emotional damage. In the meantime, the personalization technology creates echo chambers that isolate individuals in separate areas reflect only what they believe in. They would not be able to see opposing opinions, which is vital to form a balanced opinion in public debates. It leads to the spread of polarization and false beliefs, which threaten democracy and society's stability.

The current legal approaches fail to introduce an effective solution to the online privacy problem. They try to find a solution that can prevent privacy erosion without affecting an individual's autonomy. While online privacy suffers from significant violations that call for intervention, coercing privacy would lead to severe damage to the data market. Moreover, empowering users with a bundle of rights is ineffective due to the complexity of online privacy. Most online users lack the required capabilities to use those rights. Most people either are not aware of privacy implications or undermine the risks. Therefore, another strategy has to be implemented to rescue privacy.

In this study, I argue that libertarian paternalism theory offers a robust solution to the online privacy dilemma. It aims to architect the privacy choices in a manner that nudge people to protect their privacy without omitting any options. People act irrationally regarding their online privacy due to several influences factors. Those influences are inevitable, and they are being misused by companies. Nonetheless, those influences can be reshaped in order to change people's behavior in a privacy-friendly manner. Users would have all available options, but the nudge will try to alter their decisions. Privacy by design and by default, timer nudges and profile nudges are some examples of nudges that can promote privacy without imposing any economic burden on stakeholders. They are some projects that future work can build upon. Finally, nudges could work not only with users, but also with corporates. They can be designed to target tech companies in order to change their behavior, which requires further research.