Spring 8-20-2022

Surveillance Culture and Potential Resistance of Social Media in Egypt

Dina Refaei
The American University in Cairo AUC, dina_refaei@aucegypt.edu

The American University in Cairo

School of Global Affairs and Public policy

Surveillance Culture and Potential Resistance of Social Media in Egypt

A Thesis of Journalism and Mass Communication

in partial fulfillment of the requirement of the degree of Master of Arts

Submitted by

Dina Refaei Mohamed Mohamed Ali

Under the supervision of

Dr. Rasha Allam

Associate professor, Department of Journalism and Mass Communication, School of Global Affairs and Public Policy

(Spring, 2022)

ACKNOWLEDGMENT

First and foremost, I would like to express my gratitude and appreciation to my supervisor, Prof. Rasha Allam whose guidance and support has been of a great help throughout the period of writing this thesis. Your wise counsel and generous encouragement made this a very enlightening experience for me.

I would also like to thank Prof. Hesham Dinana and Prof. HebaTuallah El Shahed for being members of my thesis committee. Your insightful comments and contribution have been absolutely invaluable.

I would like to thank Dr. Shahira Fahmy for her unconditional support and trust. Your words has always been encouraging, and I was truly blessed that I have had the chance to be your student and TA for four semesters.

To my dearest mother, my role model and everything in my life, who always believes in me, whom without your support, unconditional love, this would have never been a reality. Your guidance, kindness, and your devotion has always been and will always be my greatest source of inspiration.

I also want to express my heartfelt gratitude and profound thanks to my wonderful MA colleges Salma Adham, Mohamed Salama, Passant Halwa, Toka Omr, Alaa Mahmoud and Hend El-Behary.

To my coach, Mahmoud Salem, thank you for support and encouraging in tough time in my life, I am glad I have had the chance to meet and be a trainee with you. You are truly an inspiration.

Abstract:

Social media companies have become dominant over their users. With digital capabilities that enable them to monitor, analyze and process users' data, they are able to restrict users' activities in accordance with their own policies. The present study examines the potential for users to encounter social media policies – specifically, privacy and content moderation policies imposed over activities on these platforms. The surveillance culture model is proposed to highlight surveillance perceptions among users and determine the factors that might affect users' intention to resist social media policies. A sample of 547 Egyptian social media users were surveyed. The findings showed that aware of relevant laws does not influence the user's perception of privacy on social media platforms. Instead, users assume that social media are monitoring their activities online for commercial purposes and to increase profits. While the majority were not subjected to the consequences of perceived policy violation, they are uncomfortable being surveilled. Further, perceptions of the reasons behind surveillance were found as a strong determinant of users' concerns. Moreover, the findings highlight that an awareness or perception of surveillance does not relate to mitigating behaviors by users to resist or neutralize the effects of surveillance on them. Rather, social media surveillance is considered more as a pervasive phenomenon.

Keywords: social media policies, privacy policies, content moderation, surveillance culture, resistant.

Table of Contents

List of Figures

List of Tables

List of Acronyms

AI: Artificial intelligence

CDA: the Communications Decency Act

CAPMAS: Central Agency for Public Mobilization and Statistics

EU: The European Union

IP: information privacy

META: The company owns Facebook, Instagram, and WhatsApp, among other products and services.

ML: Machine learning

NSA: The US National Security Agency

SNS: social network service

I. Chapter One

Introduction:

It is not a surprise for social media users to receive internet ads that match their interests immediately following a conversation with a friend on a social media platform. This is a common occurrence someone might notice in their daily routine. Another notable online occurrence in the current digital environment is to receive warning after sharing or posting certain content seen as violation of a platform's policies. Sponsored posts with the same products appear on your Facebook news feed, or perhaps notifications from cafes or restaurants close to your neighborhood. Initially, one might have been surprised to know how everyday activities had been recorded ; it is like a police probe. Today, it is well known that it is a marketing mechanism deployed by some social media platforms to target potential customers or curate content. However, these strategies include unprecedented and highly significant modes of surveillance. The flip side of the story is the rapid rise of the data exhaustion business model where Facebook and Google discover how to make money by selling the surplus data produced by communication and transition to third parties. Close monitoring of "smart devices" from wrist watches to vehicles, health, learning, and entertainment, is intensifying and expanding surveillance and making it virtually unavoidable (Bennett et al., 2014). Gaining social recognition by exposing one's life to the public, scoring 'likes' and 'followers' or even a comment, has become increasingly important, further promoting the idea of sharing (Srnicek, 2017).

Social media platforms are acting as intermediaries for a two-sided market; users for whom a service is provided 'for free' and advertisers who receive different advertising options

for certain categories of customers, (Evans & Schmalensee, 2015). Indeed, the amount of user-generated content through attracting active users on platforms is what defines their power in the market. Platforms are essentially "selling the user's attention to advertisers," (Wu, 2017). The more active users the platform has, the more profit from advertising it gains.

Edward Snowden's spying leak revelation (Corera, 2013) unveiled the extent of surveillance, prompting users to realize how their information might be used by third parties. The US National Security Agency (NSA) and the UK's Prism surveillance program have direct access to the data of users from nine internet firms, including Facebook and Google (Gellman & Poitras, 2013). Despite protection of the First Amendment of the US constitution for social media platforms, the regulation of the Investigatory Powers Act (2000), the prevention of Terrorism Act (2005)_, and the late Draft Investigatory Powers Bill, are all aimed at enhancing and extending the government's capacity for targeting communication surveillance on mass level. Fuchs (2015b) pointed to Snowden's revelation as it showed "the existence of surveillance-industrial internet in which capitalist and state interest party converge."(p.7) Snowden demonstrated state and corporate collaboration n in big data surveillance, while social media corporations play a crucial role in policing the internet, (Hintz, 2014; Lyon, 2014).
In 2018, five years after Snowden's leak, Cambridge Analytica; unlawfully gained access to more than 50 million Facebook users' personal data. Through the "This is your digital life" app developed by psychologist Alexandr Kogan of Cambridge University, "psychographic" profiles of people were deployed to shape users' political views to support Trump's 2016 election in the US and the Brexit vote in the UK(Farr, (2018). According to David Vladeck, Director of FTC's Bureau of Consumer Protection: "There should be little doubt that Facebook user data sharpened

Cambridge Analytica's algorithms, which made the Trump campaign's micro-targeted messaging more effective," (Vladeck, 2018).

Artificial intelligence capacities of social media platforms enable them not only to deploy targeted messages to their users but censor former defined content on social platforms internal policies of content moderation. Social media platforms are communication gatekeepers, curating the information landscape where we live. The MENA region has witnessed some remarkable incidents of content removal; for instance, in deadly military strikes perpetrated by Israel over Palestinian territories in May 2021, Palestinians publicly complained about social media censorship of their content with panning, flagging, and blocking some accounts (Human Rights Watch, Oct, 2021).

This happened one year after the Electronic Frontier Foundation sent an open letter to stat Facebook, Twitter, and YouTube demanding them to stop silencing critical voices in the MENA region stating the lack of freedom of speech on the platforms in some countries. In 2020, Facebook disabled around 60 accounts of Tunisian activists and journalists, anti-Al Assad campaign page was also disabled citing terrorist content. Similarly, YouTube erased a number of videos that documenting the Syrian uprising against Bashar Al Assad (Al Khatib & Kayyali, 2019). Twitter suspended a verified Palestinian media agency, the Quds News Network, proclaiming it is as a terrorist group, and Palestinian social activists expressed concerns about what they called discriminatory platforms against them (WAFA, 2020). Similarly, the Twitter account of an Egyptian dissidents with 350,000 followers in December 2017, shortly after anti-Sisi protests erupted, (Eskander, 2019). On Jan 6, 2020, Facebook (via its Oversight Broad) and Twitter decided to suspend the accounts of former US president Donald Trump following the insurrection in the U.S. Capital.

From the user's perspective, a senior software engineer at Facebook said that users felt they are being censored, with their content subject to limited distribution and censorship. On an internal message board, the engineer shared a message stating that "as a results, users have stated protesting by leaving low approval rate at 1-star reviews" on both Apple and Google store for Facebook, Instagram and What's App, (Solon, 2021). This was in response to the deletion of hundreds of posts condemning Palestinians evictions from the Shaikh Jarrah neighborhood and the suspension of activists accounts and the blocking of hashtags relating to one of Islam's holiest mosques. The campaign decreased Facebook's average rating from above 4 to 2.2 on the App store and 2.3 for the Google store. Advertising sales dropped at least 12% in ten days following the campaign, and an internal document connected th drop in sales to reputational damage in the Middle East. (Hootsuite, 2021).

This exploratory study examines the potential resistance of public social media users at the individual level in Egypt. With the expansion of personal surveillance on social media platforms, the present study tries to provide a behavioral analysis of social media users in Egypt regarding contemporary social media policies, through measuring the relationships between surveillance imaginaries and surveillance practices. The study tries to provide deep understanding of social media users' awareness and perception of social media policies as an antecedent to the intention of being vulnerable to data collection or taking precautionary measures combat social media surveillance. Empirical data will be examined to determine how users' policies awareness 's influences users' their perceptions and willingness to share data and express themselves on social platforms, how they perceive their privacy and freedom on social media platforms as mediums for expressing themselves. In addition, the study will explore new techniques users might use to oppose social media regulation using platforms features available

on the platforms. The paper will utilize the surveillance culture with its interrelated terms surveillance imaginaries and surveillance practices approach to reflect social media surveillance normalization in daily life and possibilities to resistance to it in the Egyptian culture context. This following section includes a brief analysis of current social media polices and regulation in addition to some international laws that control these platforms, and its consequences to provide a context of the study subject, which is necessary to understand how social media policies has been introduced. A review of most recent laws and regulations of social media in Egypt; 2015 and 2018 laws adopted for the digital platforms. Then, the paper discusses literature review on surveillance in digital realm and people's role in the recent context where the users are the content generators who are able to control and choose among different platforms. We also review research that examined surveillance with different contexts such as surveillance states and surveillance society as antecedes approach to surveillance culture as theoretical framework. This paper is one of a few papers that utilized surveillance culture approach, it provided an explanation of user's response towards surveillance on social media. It is a first paper to discuss surveillance in one of Arab Spring countries which might provide an indicator of social media users' response in other countries in the Middle East and North Africa.

II. Chapter Two

Social media platforms and policies:

2.1- Social media platforms:

Throughout the last two decades, several definitions have been offered for social media platforms. Some definitions converge from the notion of information science, public relations, and mass media. It has been characterized as a tool for communication or interaction among people focusing on message construction. Russo et al. (2008) definition is "those that facilitate online communication, networking and collaboration" (p.22). Kaplan and Haenlein (2010) followed the same approach, defining them as "a group of internet-based applications that build on ideological technological foundation of Web 2.0 and that allow the creation and exchange of users generated content" (p.61). Yet, these definitions are problematic to some extent, though they can be applied on other technologies such as e-mail and blogs. For the present study, Carr and Hayes' (2015) definition of social media will be used:

> Social media are internet-based channels that allow users to opportunistically interact and selectively self-represent, either in real-time or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interaction with others.

Components of this definition delineate users' role and content contribution in socioemotional communication processes. Internet based; they are online tools that operate via internet. Distrain and persistence, the social medium provides its services whether an individual is online or offline (Steinkuehler & Williams, 2006). Social media is perceived as interactive, specifically interpersonal in nature, providing the user with a sense of interactive engagement

with others (Sundar, 2007). User-generated value: the value of social media is derived from content generated by individual users rather than organizations, or from political expression as a channel to connect with who are likeminded. For instance, a user's simple photo sharing on a website will derive user gratification from interactive comments and exchanges. A user will utilize the value of themself through medium and communication with others (Mikal et al, 2014). Mass personal communication refers to individual engagement simultaneously in mass and through interpersonal communication (O'Sullivan, 2005). With this definition Carr and Hayes distinguished between what is a social medium and what it is not, and gave an example of each. Social mediums can be social network sites (e.g., Facebook, QQ, Google, YouTube; Yelp, Pheed), professional network sites (e.g., LinkedIn, IBM's Beehive Chatboards & discussion fora), or social/casual games platforms (e.g., Farmville, Wiki "Talk" pages; Tinder; Instagram; Wanelo, Yik Yak); whereas the following are not social mediums: Online news service, Wikipedia, Skype, Netflix, E-mail, Online news, SMS/Texts, OoVoo, Tumblr, Whisper. The present study will focus on social media platforms such as Facebook, Twitter, and YouTube. Since their introduction, social media corporations have been presented as dominant global content platforms and online speech-seeking global networks for the public, which build inherently on normative values of democratic cyberspace such as free speech, participation, and individual liberty (Lessig, 2006). Twitter, in its first days, devoted a fundamental free speech standard to protect users from policing the content. Alexander Macgillivray, Twitter's chief lawyer, said "we value the reputation we have for defending and respecting the user's voice" (Sengupta, 2012), and the general manager of Twitter in the UK, Tony Wang, said that the social network sees itself as "the free speech wing of the free-speech party" (Halliday, 2012).

Similarly, Facebook's mission -now META- was to "give people the power to build community and bring the world closer together" as a public function for all communities (Perma, 2004). Beyond these beliefs, the first established global social media platforms, YouTube, Twitter, and Facebook, in the first decade of their establishment protected their users from government collateral censorship. This was demonstrated during different incidents in Thailand, Turkey, Egypt, and Libya when governments requested content removal whether for security, political, or religious reasons (Klonick, 2018; Rosen, 2013).

2.2-Social media policies and regulations:

The first decade of the social media platforms fundamentally framed internet governance around rights, classic libertarian ethos, and preservation of individual affordance of freedom of speech. Section 230 of the CDA is considered safe harbor to social media platforms because it immunizes them from legal liability (Communications Decency Act, 1996; Andrée Weiss, 2021). This amendment relied on American democratic principles to represent an extraordinary advance in the availability of educational and informational resources to its citizens. According to the amendment, this will provide users a great degree of control over the information they receive while ensuring a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity, with minimum government regulation. Among the policies to which the amendment applied, is the guarantee of the continuation of internet development and other interactive computer services and other interactive media; and the preservation of a vibrant and competitive market for internet and other computer services which would remain unfettered by Federal or State regulations, while ensuring the vigorous enforcement of Federal criminal laws against trafficking in obscenity, stalking, and harassment by means of the computer.

Further, the First Amendment incentivizes and protects intermediaries 'Good Samaritans' by blocking off offensive material. The court then recognized these Samaritans to encourage service providers (platforms) to self-regulate the dissemination of any offensive material on its platforms (Zeran, 129 F.3d at 331., [1997]). Due to the state action doctrine, the First Amendment - protecting freedom of speech and expression- does not serve as oversight on private actors like social media platforms, but the constitution in general serves as a check on the government not on private entities (Civil Rights Cases, 1883). Yet, private actors might be treated as state actors (behave as states which control their territory) under certain circumstances, which would make them subject to some constitutional conditions (Bronner, 2017). The criticism of the First Amendment is that, currently, it does not provide recourse for social media under state doctrine (Hooker, 2019).

Even under public function, as the platforms define themselves, the courts constituted that social media fit well with private actors that open for free speech because they are no longer private nonprofit channels for content (Rathmell, 2018; Putman, 2020). EU law similarly gives these platforms an opportunity to grow without State interference or excessive monitoring obligations. Articles 14 and 15 of the European Union E-Commerce Directive explicitly interdicts the EU member states from establishing any obligations or rules for platform providers.

Thus, private companies such as Google, and social media platforms like Facebook, Twitter, and YouTube, are self-regulating entities that economically and normatively reflect the democratic culture and free speech with constitutional immunity. Drawing on the First Amendment's free speech principles and EU law, some concerns were raised by the court to the platforms, which might severely restrict the number and the type of messages users create. Just

like the courts, scholars have struggled with the question of how to curate these platforms to balance users' first amendment rights to free speech against social media platforms strict control over the content.

The International Covenant on Civil and Political Rights (1966) addressed freedom of expression in article 19, "freedom to seek, receive and impart information and ideas of all kinds regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice" yet, this freedom came with some limits "… for respect of rights or reputation of others and for protection of national security or public order." International law also recognized limited freedom of speech in 1994 under article 19 "anyone shall have the right to freedom of expression but in the third paragraph some restriction was added. Some conditions should be met, it must be provided by law, it must address one of the aims enumerated and must be necessary to achieve the legitimate purpose" (Womah Mukong v. Cameroon, 1994).

Assumptions about social media openness for speech were controversial at the time ; some thought that it would enhance democratic culture with its wealth of publishing tools, while others pointed to the threat of private control over speech and cyber rights of users (Klonick, 2017). While these platforms have an upper hand on how to exercise their significant roles in this expressive world, an understanding of the motives of the business model and content moderation policies of these platforms, indeed, is needed to evaluate their impact in democratic cultures.

2.3- Self- Governance of social media platform:

The late twenties of this century vision of free expression is incapable to protect freedom of speech today (Gozalishvili, 2021). It is no longer territorial governments-citizens' relationship, it became a more pluralistic vision with multilateral governors. Balkin (2012)

described it as a three-dimensional triangle: firstly, nation states or multilateral powers like the European Union; second dimension is mediators or privately owned companies including social media platforms, search engines, broadband providers, and electronic payment systems; the third dimension, is the entity that encounters the aforementioned two: end users, citizens, speakers, legacy media and civil organizations, hackers, and trolls. This study will focus on social media companies only.

The configuration of powerful forces, where private regulation directed at speakers and both states and civil society pressuring the infrastructure owner or mediator to regulate speech, created some problems. State pressure on digital companies results in collateral censorship and prior restraint. Collateral censorship is a form of indirect censorship through liability imposed on a private intermediary to censor another private party's speech or third-party speech (Wu, 2014). Prior restraint is to describe "administrative and judicial orders forbidding certain communications when issued in advance of the time that such communications are to occur"(Alexander v. United States, 1993). Social media platforms with their opacity standards and private bureaucracy system arbitrarily govern end users ignoring democratic transparency rules. Therefore, users suffer from being vulnerable to digital surveillance and manipulation.

The new school of digital communication is directed at internet infrastructure or mediators, for instance, social media platforms (Baklin, 2013). To force infrastructure to surveil, police, and control speakers or online content creators, nation states attempt to put some regulations and threats to internet infrastructures. For instance, to limit forbidden speech, the Network Enforcement Act law (Facebook-Gesetz) in Germany was amended to combat hate speech and fake news (BBC, 2018). To protect citizens from having their private stories in online newspapers the EU created the 'right to be forgotten' which is directed at search engines

in the hopes of increasing citizen privacy. The German NetzdG law's impact in preventing hate speech remains uncertain (Echikson, 2018). After the Charlottesville protests in 2017, the law enforces some private infrastructure owners to block neo-Nazi site.

Collateral censorship or regulation of speech increasingly depends on new schools but is directly affected by old school methods of control where nation states are attempting to coerce or co-opt private owners of digital infrastructure to regulate private actors' speech. Digital prior restraint imposes liability on infrastructure providers unless they surveil and block pre-defined categories of speech (Balkin, 2017). Indeed, prior restraint, however, is not identical to the classic methods, it has some similarities or features of the past. Administrative prior restraints ignore people's right to speak unless they have the permission of a digital platform. Such digital control means nothing happens unless a bureaucratic authority decides what and when this content or words are visible to others; this process happens secretly with no transparency.

The new school of speech led to public-private cooperation and co-optation between governments and digital infrastructure. To surveil and regulate speech, governments coerce private digital infrastructure to bid and help speech regulation for some reasons. First, digital infrastructure owners have technical capabilities that far outstrip those of most countries; they easily identify and remove content with algorithms and artificial intelligence (AI) (Balkin, 2017). Second, they depend heavily on data surveillance to know what end users are doing. Third, controlling the operator or owner is usually easier for nation states because of the number of speakers and anonymity of the users. In the end, private companies want to expand their markets, reaching customers within the authority of the nation state. Nevertheless, infrastructure companies believe in users' freedom and civil liberties, the cooperation with nation states will be objective towards achievable profit-making goals.

Fourth, due to the states and multilateral powers such as the European Union's pressure, infrastructure owners seek to increase their technical capacities to meet their needs. The more powerful the technical capacities, the greater capacity they have for governance of large populations of end users. Thus, privately owned digital infrastructures such as social media platforms encourage more regulation of speech, enhancing methods of surveilling, controlling and forbidden activities on the internet. Filtering techniques developed and expanded nationally and internationally, which make it become ever more proficient to achieve states' demands (Balkin, 2018).

Technological expansion of private companies- especially social media companies- increase their capacity for surveillance and control, which can lead them to be seen as new private governance sources. They can be seen as new governors who control online speakers, communities, population, with an assumption of merely facilitating or hindering digital communication. As Kite Klonick explained, social media companies like Facebook, Twitter, Youtube created large global bureaucracies that enforced their terms of services agreement and made them stand as community values and norms. Nevertheless, these agreements had to be a combination of contract and code which had to meet states' demands.

On the other hand, the capitalist logic to generate growth and please shareholders performed through two ways; expand people's membership around the world and gain users' attention by making users addicted to their services (Wu, 2016). The business model of digital companies is built on attracting end users by offering free services in exchange for providing end users' information to advertisers. Thus, these platforms must guarantee safe communities for users and provide interesting content, otherwise, they will lose users and time spent on the platform will decrease. To sell end users' attention, collection of greater amounts of end users'

data is necessary to know things about them so that they are more attractive for advertisers. Such logic drives social media companies towards surveillance (Zuboff, 2015).

2.4-Social media policies infrastructure:

The perspective of new "internet governance" control over the content and First Amendment immunization created an individualistic approach of rules which Professor David Post called "market for rules;" each social media platform has its own policies with the same motive of profit increase based on big data. By encouraging and facilitating platform users' interaction- more posts, more liking and more sharing content and comments- platforms like Facebook, YouTube, Snapchat, and Instagram maintain their businesses. The utopian belief of "mak[ing] the world more open and connected" and not policed the content challenged (encountered) by users' expectations and profit growth for these platforms. Competing principles such as user safety, not harming users, corporate social responsibility, and more importantly economic viability, forced each platform to create rules and community standards to curate speech to meet user's speech and community norms. In the term of private self-governance or regulatory, early stages of the regulation and content moderation system of major platforms like Facebook, Twitter and YouTube were described as opaque (Klonick, 2017). They seek to demonstrate that they are working on moderating content to their users to maintain online speech. Yet, the rules cannot be presented as rules but as standards, according to which the content moderators are the only ones who can filter content or flag them (Solum, 2009).

Initially, YouTube set standards with no more than one page of information for moderators to understand what content should be removed; content such as child porn, hate speech, and abusive content following criminal laws globally. In 2009, Dave Willner with his team created the first draft of what Willner called "all-encompassing" rules for Facebook, which

consisted of 15,000 words (Klonick, 2017). Due to the rapid increase of both users and the volume of content, the spread of the platforms globally and the diversity of the online community, and the need of more human moderators with diverse backgrounds for content moderation, both YouTube and Facebook developed policies from these rough words-early system of standards- to automatically introduce today's rules.

Before discussing how these platforms govern their communities in detail, a differentiation of platform law components should be considered. Each platform sets its own policy that is composed of four main aspects: consent, common law as norms, common law procedures, and technical law.

Table 1:Elements of social media platforms policy:

Table (1)

Element	Description	Examples
Consent	is a contract between users and company which governs the respective rights of each of them	Term of services (ToS)
Common law (Norms)	Community standard, rules or policy rationale with explanations of policies and actions.	● Warnings, notices, explanation of some measures which are sent to users ● community standards or rules (including policy rationales and examples
	Content moderation and users' activities (Decisional Claw)	● Content remove or allow decisions, when and how to sanction users ● Decisions made on certain appeals ● Decisions on content such as nudity or religion.
	Guidance for Internal policies used to moderate content and govern user account suspension and termination	● International police and documentation ● Moderators' training
Common Law (procedures)	The steps taken to execute the law Flagging, reviewing, removing content and sanctions	● User flagging ● Algorithmic flagging ● Community moderation ● User moderation ● Procedure and criteria for escalation and sanctioning ● Appeals processes
Technical Law	Technical and system design choices	● What kinds of posts are allowed (links, text, photos) · How much content is allowed · Real name requirements · Algorithms for content moderation · Mechanisms that feed into algorithmic preferences (likes) · Tools for sharing content (retweets, shares) · Tools providing users with control over content

2.5- Content moderation:

Content moderation could be defined as "the process of screening and evaluation of the user-generated content posted by users on websites, social networks or other digital platforms." This process is ideally to facilitate cooperation with users and prevent online abuse. However, digital communities initially relied on volunteer moderators, commercial content moderation is done by subcontractors to gain money and make profit (Çömlekçi, 2019). With the growing exponential amount of user-generated content, in 2009, content moderation by humans only has become an impossible mission for platforms (Ofcom, 2019). Hence, the moderation process happens at many levels; ex-ante moderation which happens before publishing, ex-post moderation which occurs after publishing, by humans or automatically with algorithmic methods such as PhotoDNA, Geo-blocking and Content ID in addition to all feature mechanisms for users to report, spam or flag content manually (Klonick, 2017). A new method of content moderation has been shaped using machine learning (ML) and algorithms. Such systems are meant to optimize the speedy detection of potentially harmful content. ML) and algorithms. Such systems are to optimize the speedy detection of potential harm content.

However, the technical meaning of "harmful" content changes depending on what the function or purpose of the platform is and its own contractual standards, for instance, Facebook has its own community standards along with methods to ensure users compliance with legal requirements of their region. Platforms made use of ML to flag and remove some types of hate

speech for instance. Others are based on prediction and prevention to spot objectionable content before it is seen by training ML algorithms, which YouTube initially used (Katsh & Rabinovich-Einy, 2017). Furthermore, Zhang and others (2018) asserted that platforms seek to predict and prevent some behaviors that have never occurred based on real time data on uploaded users' content. "Takedown and stay down" has been deployed by these platforms to actively monitor new uploads to ensure that similar content will not be reloaded after removal (Bridy, 2016).

However, ML control over substantial amounts of user generated content raises serious concerns from a social welfare perspective (Bamberger, 2010). According to Elkin-Koren (2020), online content moderation has become ubiquitous. The new way of governing speech, using ML, challenges the main principles upon which public spheres in democratic societies are built. Digital platforms facilitated a new online discourse which constitutes the modern public sphere (Presuel & Sierra, 2019). Justice Kennedy of the Supreme Court of the US described it recently as:

> While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the 'vast democratic forums of the Internet' in general, and social media in

Yet, numerous scholars demonstrated that the neutral infrastructure of online platforms has been far from an intermediary where all can express themselves and where it merely connects varied users' views (Gillespie, 2018; Suzor, 2019). The content, through data driven microtargeting, is tailored to each individual which shapes the public sphere (Bodo et al., 2017; Gillespie, 2018). Balkin (2016) explained that the platforms are enabling content with the impending spread of unwarranted speech while occasionally restricting desired speech,

(Langvardt, 2018). Due to the optimized design that gives them the capacity to allow or pre limit content uploading, platforms decide what should remain or be removed and limit who can participate in online conversations and who would be likely to watch certain content through algorithms (Evans & Schmalensee, 2016). Such speech control is driven by the economic interests of these private platforms; hence, they constitute the digital public sphere (Plantin et al., 2018).

To discuss content removal, it happens through many mechanisms and for varied reasons. Common good, legal norms, and free marketing approaches are shaping content moderation processes. Elkin-Koren (2020) argued that not only is filtering out shaping the public sphere but it also determines what remains available for public consumption. Moreover, the democratic ideal assumption of self-governance provides people with the impression that they have access to information that allows them to make their own decisions collectively and decide their common destiny. Yet, the removal of content from the public sphere without accountability may silence minorities or people with different points of view. As a result, some people may deprive themselves of legitimate speech.

Removal of content out of legal duty or informal governmental restrictions may also restrict speech in some authoritarian countries. Some public authorities might nudge these private businesses to perform law enforcement tasks. Consequently, regular content might be removed intentionally and unjustifiably, resulting in high levels of censorship (Heldt, 2019). Therefore, in authoritarian countries. Therefore, in authoritarian countries, filtering will ensure that free speech cannot be guaranteed and that users' interests will not be protected Furthermore, invisible foundations of content removal and filtering remain controversial, unwarranted content

(such as copyright infringement, hate speech or terrorist propaganda) definitions are concealed in machine learning code (Grimmelmann, 2015).

Free market has an impact on content moderation as well. Since these platforms are assumed to be "marketplaces of ideas" which are free to deploy content moderation policies without any governmental interference. users can distribute content or distinguish and select what type of content accommodates their preferences under section 230 of the First Amendment of the CDA 1996 - and in democratic spheres. Yet, the concealed definition and opaque ways of content removal on social media platforms will restrict users' capability to offer accurate signals to perform their roles as a content creators or generators whether to flag content, mark it as spam, or choose their preferences. Therefore, the assumption of a competitive marketplace of ideas has become dysfunctional.

Many incidents showed AI failure to reflect public interest. According to the nonprofit The Counter Extremism Project stated that Facebook has failed to track and remove well known Islamist extremist propaganda. Similarly, YouTube with its ML system had erroneously deleted more than 100,000 videos which reported on chemical attacks and human rights violations in Syria. Recently, Facebook, was also accused of allying with Israel against Palestinians; "7amleh", a Palestinian digital rights non-profit, documented more than 500 removals on Instagram and Facebook between 6 and 19 of May 2021 (Paul, 2021). The US congresswomen Rashida Tlaib wrote "I cannot understand how Facebook can justify censoring peaceful Palestinian voices while providing an organizing platform for extremist hate." (Paul 2021). The number of posts and content removed after shaikh jarrah eviction has been highlighted the

amount of censorship of Palestinians content and to what extent Facebook's opaque decisions as a mediator is shaping what information comes out of a war zone.

2.6- Social media platforms, privacy and personal data use:

Social media use simple forms of consent based on the principle of respect for autonomy, which put individuals as the centers of control over their own lives and data. Based on informed consent, social media processes a large number of users' personal data. Social media users theoretically make their conscious, rational, and autonomous decisions to share their personal data in the digital sphere, though, the freedom of choice to practice this right is questionable. Although it seems that people can manage their information and self-representation by controlling context and audience, it is difficult for the users to determine or decide how social platforms moderate content. Due to social media networks' aggregate context and tailored content (Hargittai & Litt, 2013); they do not fully understand the consequences and risks of data processing.

Previous studies provided insights into the user's capacity to understand their consent to privacy policies. A study that analyzed privacy policies in eight different SNS websites and users' expectations of these policies showed that policy readability is extremely low and there is a significant dissatisfaction with current privacy practices of social media websites. Data controllers focus on complying with regulation that exist in each region rather than users' needs, interests, and preferences (Custers et al., 2014). More legitimate demands arose concerning online privacy (Bashir et al., 2015), the results of two-part privacy surveys to assess users' knowledge and opinion of online privacy practices showed that respondents lack sufficient comprehension of main privacy issues stated in platforms consent forms, and that most

respondents have been coerced into submitting their personal data online.

People's concerns have an impact on information sharing. A survey analysis by Jeong et al., (2017) highlighted a positive relationship between privacy concerns and trust of platforms and willingness to share information. However, users believe in the function of social media sites to protect their information, extremely concerned people are less likely to share information. Further, the more the users are aware of privacy policies, the more the users tend to maximize privacy features that social platform are functioning to decrease data hacking on their platforms. As a result, they will behave more carefully in the digital environment (Tuunainen et al., 2009).

2.7- Social media in the Egyptian context:

Social media platforms have a substantial impact in the Arab region. Citizen's usage of Twitter, YouTube, and Facebook helped in planning the uprising against the former Egyptian President Hosni Mubarak in 2011, garnering attention and support for the Egyptian people around the world. Strikes across Egypt brought daily life to a halt and toppled President Mubarak. Digital platforms facilitated and escalated the movements and mobilization against Arab rulers at the time. In Tunisia, late in 2010, calls escalated for the restoration of the suspended constitution of the country. Meanwhile, provincial Libyan leaders sought to strengthen the newly independent republic. This was an unprecedented result of the growing businesses of social media platforms in the Middle East media platforms in MENA, following the trend of the launch of Facebook Arabic interface in 2009.

The platforms continue to see a significant rise in numbers from ten million in 2010 to 254.94 million in 2020. This paper focuses on the Egyptian context. In January 2022, out of Egypt's total population 105.2 million, there were 51.45 million social media users representing

48.9 percent of the total population (Global Digital insight Report, 2022; CAPMASS, 2022). Meta's resources released that Facebook's users in Egypt were 44.70 million in early 2022, and Google in its update indicated that YouTube has been used by 46.30 million in Egypt. Whereas Facebook Messenger reached 34.60 million, Instagram had 16.00 million users, and the most recent app TikTok had 20.28 million. (Global Digital insight Report, 2022). Meanwhile, Snapchat had 13.60 million and Twitter had 5.15 million. Due to the rapid expansion of social media and its ongoing influential role in political mobilization, the Egyptian government realized the importance of these platform for understanding and improving government – citizen relationship moderation.

After the 2011 uprising, the media landscape witnessed significant structural and legislative changes. The Egyptian authorities put more restrictions on social media and online space in general, within broader government domination and social media monitoring. In 2014, a systematic plan was announced to monitor social media platforms, Egypt bargained with US-based company Blue Coat which started to monitor Egyptian online communication putting the social media sites under surveillance (Ahram Online, 2014). Counter-terrorism Law 2015 (law 151) and Cybercrime Law 2018 were issued in order to limit the spread of false news and misuse of social media. The laws gave the state the power to block and penalize social media accounts (Reuters, 2018). Under these laws, social media accounts with more than 5,000 followers are treated as media outlets and are subjected to prosecution for publishing false information or breaking the law. Yet, those laws have been widely criticized for expanding government control over social media: "the vague wording of the law allows authorities to interpret violations and control the media" said Sherif Mansour, Middle East and North Africa Programme Coordinator

for the Committee to Protect Journalists. Whereas it has been seen as pivotal to compact and limit digital platforms' misusage (Abdel Meguid, 2020; Badr, 2020).

The outbreak of COVID–19 worsened the situation when the public prosecution office announced in March 2020 that false information spread might result in a fine of 20,000 EGP or put social media users at risk of imprisonment (Al Ahram Online, 2020). Following the prosecution announcement, authorities blocked several social media accounts with no justification. Further, personal data is by default accessible to national security bodies. The 2020 Personal Data Protection Law no. 151 article 3 enables national security bodies to possess all personal data without legal justification. It was the strongest tool used by the Egyptian legal framework to abuse digital rights during COVID-19 (Farahat, 2021b). The existence of laws on the protection of privacy does not guarantee a fully secure social media landscape for users. Cybercrime Law, article 2, puts a restriction on service providers to retain, restore, and record information in their systems for a period of 180 continuous days. Thus, the current law also expands authorities' surveillance on social media platforms which led to tracking COVID-19 information and cause many arrests on the account of circulating fake news (Farahat, 2021b; Hassanin, 2014). The annual report on freedom of expression stated that these "measures were to direct online users towards a sort of self-censorship" (AFTE, 2020a).

A Research conducted by Open Technology Fund Information Controls highlighted the strategies used by the Egyptians security to surveil citizens on social media platforms through an array of technically unsophisticated mechanisms, including device seizures and searches, informant networks, and surveillance of publicly targeting available social media content. Further restrictions were deployed through the government narrative for discrediting rightful

digital expression. Social media has been used extensively as a propaganda tool for the governmental narrative. As Larry Diamond (2014) argues, “authoritarian states . . . have acquired (and shared) impressive technical capabilities to filter and control the Internet, and to identify and punish dissenters.” The digital platforms, moreover, played a vital role in mediating the communication environment. New citizens and different public spheres could have ambiguous and contradictory effects, yet authoritarian regimes could adopt and absorb these changes (Lynch, 2011). Citizens, in the end, are under surveillance from both governments and social media platforms themselves for varied reasons. For this study, the rise of citizen response for this kind of surveillance is examined to highlight the potential resistance against digital surveillance.

III. Chapter Three

Literature review:

3.1-Perception of surveillance in the digital realm:

There is no prospect of mass surveillance on the internet being accepted by all, or even of being abandoned by any authorities in any nation states. Yet, the question here is, what do online users know about surveillance? How do they perceive surveillance as the subjects or objects of that surveillance? Which surveillance methods or purposes are more acceptable to them? An argument over surveillance is still under investigation by many scholars. There are many critics and ongoing discussions over two opposite issues such as privacy and security patterns. Data gathering and surveillance portrayal have an impact on individual perceptions of surveillance, individual rights, and freedom of speech in the online realm.

Surveillance on social media is embedded through the algorithms, consequently, it allows them to exercise an unprecedented degree of control over individual communication. As discussed above, social media platforms can more preemptively determine what kind of speech should be permitted and which should be suppressed, according to vague criteria created by their own commercial priorities and incentives. Algorithms augmented the existing power of these platforms, a process characterized by a high potent

A study by Afriat et al., (2020) that examined the youth rationale of Facebook surveillance in Israel, before and after the Cambridge Analytica scandal, revealed a shift in the youth's perception of privacy. A marked shift happened among the respondents. Their understanding of privacy as a concept, from being a commodity or trade off– having personalized digital services in exchange of information disclosure – to advancing their own

perception of privacy as a human right in which one needs to accept or reject participation in; seeing surveillance as inherent in society emerged with the digital world. However, the result of the analyses underscored social media as an integral part of todays' life; some of the young adults among the participants' suspect their ability to delete the application in contrast to their contention to not being under surveillance.

Concerns over privacy increased as well. The former study aligns with previous research where the participants were more concerned with their social privacy rather than institutional privacy. For instance, Stutzman et al.,(2013), show that users, by changing privacy settings, tried to increase their level of social privacy, while sharing more personal information. Since they are not fully aware that they are sharing this information with silent listeners. Stutzman et al., (2013) highlighted that the amount and the scope of the personal information that Facebook has been indirectly revealing to advertisers and third-party apps markedly increased in the study period 2005-2011. Draper and Turow (2019) stated that social media users who are aware of mass surveillance might care about its repercussions. Thus, users face some challenges in managing their privacy settings. At the same time, they are powerless to affect information disclosure and their privacy behavior in comparison to the power of providers of social media services.

3.2- Self-inhibit free speech and Behavior:

In the second decade of the 21st century, a significant body of research was conducted to address social consequences on social media users who thought themselves suspects of data surveillance. Bauman et al. (2014) discussed:

> What is clear is that the subject of surveillance is now a subject whose communicative practices are seen by the surveillance agencies as of potential informational value or

> utility, where this value might be related to security or the economy. [.....] As the subject communicates in cyberspace, there might be some awareness that the communication network is variously being monitored, registered, stored; however, there is a lack of knowledge as to the informational utility accrued to that communication by the surveillance agencies.

Similarly, an investigation on the implication of pervasive surveillance on state–citizen power shifts raised questions about citizen capabilities to participate in the digital environment. It showed to what extent public debate, knowledge, feelings of disempowerment of citizens, and state corporate interest dominated and control over those citizens (Isin & Ruppert, 2020). Furthermore, after Snowden some studies found that social media users have expressed concerns, confusion and significant levels of unease to understand how data is generated and collected, by whom and for whom it has been used and how users can address these challenges (Eurobarometer 2015; Information commissioner's Office, 2015).

Some activists realized the drawbacks of surveillance realism. Dencik and Cable (2017) highlighted it to policy makers and courts in democratic countries. Public citizens, in turn, have been familiar with personal data collection on social media platforms and online activities. A survey of writers revealed, out of individual's awareness after Snowden, citizens' reluctance to engage in sensitive political topics online, with a significant decline in privacy sensitive search terms on Google (Marthew and Tucker, 2017), as well as page views of terrorism articles on Wikipedia (Penney, 2016). In a nationally representative sample of Taiwanese people, Ping Yu (2021) found a positive relationship between political expression and Facebook privacy management openness, and a negative one with the acceptance of online government surveillance. Some minorities stopped expressing their political point of views on social media (Stoycheff, 2016). Spirals of silence debates spread widely on social media as well. The chilling

effect of surveillance awareness has been found as a repercussion of people merely being aware of online regulations, others scarcely hypothesize different surveillance scenarios. As Greenwald (2014) discussed, “mass surveillance kills dissent in a deeper and more important place as well, in the mind, where the individual trains him- or herself to think only in line with what is expected and demanded” (pp. 177–178). Such an approach can be explained with the chilling effect in literature where people were afraid of legal prosecution and were uncertain of the process. A clear example was seen, according to Solove (2006, 2007), after 9/11 when surveillance was introduced explicitly as an inhibitor of people to legitimate and acknowledge the feeling of indirect risk among the public.

Moreover, the reasons behind responses to surveillance, according to Cobbe (2020), will vary; some individuals may escape from corporate or state monitoring, others might change their language or words. Everyone has his own style of resisting. Indeed, one might have many reasons for resisting or encountering digital surveillance. For Cobbe (2020), resistance could be conditional or contextual, in other words, temporally for a defined period of time, or spatially on certain platforms. It may be contingent or may vary in its strategies and practices.

3.3-People's sense of practice:

Understanding of contemporary surveillance methods and its consequences on individuals has been studied in many fields. Following Lyon (2017) approach, Jamie Duncan empathized with the citizen’s role to renegotiate the inevitable ubiquity of technologies like Big Data in commerce, politics, and social interaction. However, such a participatory role of citizens could not be enacted without transparency, knowledge to set themselves accountable to protect their data. Thus, digital citizens could construct and socialize as subjects who understand online

participation and are aware which information can be bought, sold, and leveraged for control. In an environment where there are inherent relations between government and corporations such as social media platforms ordinary people are under social and political risks from a new posed policy challenges related to transparency, inequality, and civil liberties.

Sets of social practices can be distinguished based on varying degrees of individual consent and agency. Scholars such as Lupton (2014) differentiated between participatory and voluntary surveillance practices or what is called by Lupton (2014) as "social media surveillance implication or the self-tracking practice, " (Marwick, 2012). Similarly, the implication of social surveillance resulting from the use of social media, was described by Lyon (2017) as responsive and litigatory surveillance practices. For Lyon, responsive practices are the "activities that relate to being surveilled and the initiation practices are the "modes of engagement with surveillance". Yet, Barassi later agreed that under data surveillance or "datafication" each form of digital participation is, at least, partially 'coerced'. In a diverse context, with a sample group of adults who identified as Muslim in America, Stoycheff (2019) demonstrated a relationship between higher perception of online surveillance and a likelihood to engage in illegal activities but deterrence to engage in legitimate political participation online. More recently, surveilled individuals' practices were examined in the Swedish context and it was found that respondents tend to encounter surveillance by self-censor; not sharing private information, deactivating certain services for encryption and anonymization, and disabling location services. Half of the respondents avoided using some app because of data gathering policies, around 60% of the respondents disabled their location defining (Cocq, Gelfgren, Samuelsson, & Enbom, 2020).

To conclude, an individual's increased sense of surveillance on social media at the personal level could be explained through many approaches. Due to varied causes of surveillance

(imaginaries) on these digital platforms, people's perception of being subjected to it or not is based on their awareness of how these platforms– with their automated, continuous, and unspecified collection, retention, and analysis of their personal data– will use the collected data. The cultural aspect of surveillance has inevitably impacted communication practices, the context of lack of transparency and freedom of speech in the community where individuals may be surveilled, gradually normalized surveillance practices, or led to resignation despite unease (Dencik & Cable, 2017; Smith, 2018). Individuals, indeed, in a specific population will have varying preferences in a position of control regarding trading their own data according to benefits they might receive (Draper, 2017).

IV. Chapter Four:

Theoretical framework:

4.1-Surveillance culture:

Surveillance is defined, in the Oxford dictionary, as " the act of carefully watching a person suspected of a crime or a place where a crime may be committed" and, in the Cambridge dictionary, as "a careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected". Yet, in academic scholarship surveillance is more about power implementation and performance of the more powerful in a relationship. It could be pronounced in statuses and hierarchical levels. A clear example is institutional power over institutional actors. Surveillance originated in sociology; however, it has been traced by James Rule (1973) to define the way by which large bureaucracies practice data collection to invade privacy and maintain social control over their individuals.

Surveillance can be defined as "the systematic monitoring of people or groups to regulate or govern their behaviors." (Esposti, 2014). Surveillance understanding, however, stems from dystopian literature such as George Orwell's *1984* and *Minority Report* by Steven Spielberg. Throughout history, it has been thought of in different contexts. Firstly, Jeremy Bentham's panopticon prison model where "all prisoners are made visible from the center tower while the guards cannot be seen." Then, the panopticon model developed by Foucault (1977), became all-encompassing surveillance where inmates are uncertain about when they are being watched by the guards. This led to self-scrutiny, individuals become their own watchers and police their own behavior, they are aware that their lives are visible to others. Surveillance is a transdisciplinary issue, represented in sociology, political science, criminology, anthropology,

geography, philosophy, communication, media, and information studies. This led to the rapid advance of empirical studies. Criminology studies of personnel operating public areas and closed (Sutton &Wilson, 2003). Fussey (2007) focused on the police's support for the development of CCTV implementation in some political conditions, highlighting the motivation and intention behind camera operation in certain areas.

In addition, Lyon (2001) worked on positioning surveillance in the spectrum of "care "control" for watching to protect people or to enforce discipline. This was a turn in surveillance studies; researchers (Nelson & Garey, 2009) noted that surveillance's effect and experience differ according to purpose, setting, and population. Moreover, social sorting has been practiced, based on distinct categories of populations with unequal regulation of people's mobilities and monitoring of people for public services. Surveillance is no longer for security only, but it has been accelerated for commercial values with negligible risk such as screening and preapproval of cameras at airports, at home, and inside workplaces (Graham & Wood, 2017).

With a focus on communication, in the late 1990s, William Staples (1997) focused his attention on systematic data collection of individuals by organizations to maintain social control. This was developed later by Haggerty and Ericson (2000) as "the surveillant assemblage" which is defined as the information systems that people are directly exposed to while creating "data baubles" upon which some organizations act. Like what usually happens in the workplace and institutions or organizations by camera monitoring in all sites.

Technology facilities encouraged personal information broadcasting to an intangible network of audiences that include friends, employers, and family members, even people who individuals have never known or met before (Duffy & Chan 2019), which changed the context of surveillance. Thus, some scholars consider this the digital transformation of

societies, describing it as “forms of monitoring of endemic digital society”. Mark Andrejevic (2005) called the surveillance world of watching one another “lateral surveillance” in which individuals lived in a savvy and skeptical society where they adapted some practices to gain information about friends, family members, or loved ones. The article discussed technology adoption such as cameras or X-ray glasses with an ideology of “responsibility” to save society and consume these services to monitor one another.

The new grounds for communication created by social media platforms led to repositioning the users in a responsive role; as Jonathan Finn wrote in his book “surveillance has become a way of seeing, a way of being” (2012, p 78). As subjects who can evaluate and affect the whole communication process. People can actively participate in regulating their communication environment in an unprecedented culture that has emerged with social media open networks. The proposed model for this study is the “surveillance culture” model built conceptually on Charles Taylor’s work (2004), and surveillance practices to understand today's interconnected world in which surveillance becomes a central organizing feature of the digital information infrastructure of societies. Rather than a surveillance society and surveillance state, David Lyon (2017), distinguished a new key feature of surveillance culture is the participatory role of the subjects who initiate, negotiate, or resist this surveillance.

Surveillance could be defined according to different contexts and practices for several reasons, such as police practices (Marx,1988), and at the micro-level like managing one’s identity whether for personal relations or employment purposes (Duffy& Chan, 2019), or at Massa level as data processing through social media platforms as we see today. Yet, the main logic of old and modern surveillance is gathering personal information and data collection. The

concept of surveillance traditionally was about institutions such as government and corporations enacting it to have control or power over individuals, (Ball, 2010).

In the context of online social networks, in the first decade of the 21st century "Participatory surveillance" was conceptualized as a form of empowerment and sharing. Anders Albrechtslund (2008) highlighted the potential dangers of surveillance on the Web, since then privacy and transparency concerns have risen. Concerns were against the trading or commodification of personal information. To make it simple, sharing information means it could be used for corporation marketing which targets individuals according to search keywords on their browsers.

Meanwhile, an original approach to surveillance was hypothesized by Gary Marx in 2016 when he stated "surveillance implies an agent who accesses personal data" however privacy "involves a subject who can restrict access to personal data through related means" (p.23). Both the assumption of data retail and one's effort to have control over their data involve the concept of power or influence of one entity over the other (Humphreys, 2011) (p.256). Hence, the individual's awareness of being monitored by social networks remains largely skeptical for scholars.

Imagined surveillance has been introduced by Brooke Erin Duffy and Ngai Keung Chan (2019) to describe "how individuals might conceive of scrutiny that could take place across the social media ecology and, consequently, may engender future risks or opportunities." Accordingly, some responses might be the result of imagined scrutiny which includes disciplinary and anticipated resistance tactics, such as the use of privacy settings, self-surveillance, and pseudonymous accounts.

However, the understanding of imagined surveillance among individuals on social networks depicted by Andrejevic's study on self-presentation of youth among 18 and 24 years old on different social media platforms such as Facebook, Instagram, LinkedIn, Snapchat, and Twitter. "You never really know who's looking" has become a common statement amongst internet users. Imagined surveillance across social media platforms revealed that young generations is aware, to some extent, of creating an identity for themselves on the internet for their future employers. The assumption of being watched/monitored on social media is understood by younger people; however, it is a relative phenomenon between oneself and the followers on their account, the people on one's network whom they give direct access to.

4.2-Culture of surveillance in the context:

The surveillance culture as a framework cannot be separated from the assumptions discussed above, but it is analytically distinguishable with its two pillars: surveillance imaginaries and surveillance practices. Lyon (2017) tried to argue surveillance is "a part of the whole way of life" that can further describe social media platforms' prescription for users to increase engagement levels through sharing and making themselves more visible. For Lyon, culture is defined as "something those everyday citizens comply with—willingly and wittingly, or not—negotiate, resist, engage with, and, in novel ways, even initiate and desire." Such an institutional aspect of technology that is internalized, shapes parts of daily life practices and enhances a social control or discipline mode or what was described, later, as a post-Snowden world where digital modernity mediated citizenship and surveillance.

In contrast, firstly, the culture of surveillance happens at a mass scale which changes the surveillance dynamics from the past; no one is exempt from its detrimental impact (Lyon, 2017). Secondly, a great amount of this data is generated by millions of ordinary citizens' activities online. Thus, citizens or users of social media platforms never cooperate in their surveillance by sharing at the same time. Social platforms are based on citizens, consumers, or even employees' experiences and engagement with this surveillance. One of its characteristics is its relation to the global political economy, as argued by Shoshana Zuboff, and the emergence of surveillance capitalism which directly involves big data practices (Zuboff, 2016; Lyon, 2014a). Its goal is to predict and modify human behavior to generate more revenues and control the market (Zuboff, 2015, p. 75). An analysis of Google's strategies by Zuboff (2015) provided evidence of "formal indifference" towards others' base, which is related to the surveillance culture that Google seeks to grasp certain users' responses to predict and adjust their behaviors online which will affect the corporation's success. Furthermore, surveillance culture is like any culture, it has many facets and varies according to region (Lyon, 2014). Therefore, this culture will be affected by the context where there is unpredictability and increasing social liquidity (Bauman & Lyon, 2013). For Bauman, "liquidity surveillance often found in the consumer realm that spread in unimaginable ways, spilling out all over" (Jurgenson, 2013).

4.3-Surveillance imaginaries and practices:

"Surveillance imaginaries" are typically constructed through everyday involvement with surveillance and include a growing awareness that one's whole life is under surveillance. This affects social relationships in diverse ways. For instance, how a future employer may look at one's account on Facebook. Thus, imaginaries, according to Lyon, offer "not only a sense of

what goes on—the dynamics of surveillance—but also a sense of how to evaluate and engage with it—the duties of surveillance," in turn, it "informs and animate surveillance practices," both belong together. On the other hand, Surveillance practices "maybe both activities that relate to being surveilled (responsive) and also modes of engagement with surveillance (initiatory)", (Lupton, 2014).

4.3.1-Pervasive surveillance:

According to Foucault, states and institutions maximize efficiency by putting the subjects in a state of permanent visibility, a novel panopticon ideal way of maintaining control. Similarly, current surveillance in the context of social media has become so pervasive that the majority comply without questioning it (Zureik et al.,2010). Contemporary surveillance with widespread social media platforms, for instance, will puzzle people who used to live under authoritarian regimes (Bauman & Lyon 2013). Users could not easily figure it out since they have been living for decades under the same sort of monitoring. Yet, Lyon (2014a) explains it through three commonplace factors: familiarity, fear, and fun.

Familiarity, in general, surveillance could be found where people take it for granted as an aspect of their life, such as cameras in private and public places, security check routines in airports, and other sites. Watching has become "a way of life" for people who are fed up with being monitored in all their interactions (Longhurst, 1990). A content analysis by Jorgensen et. al, (2016) outlined the tension between journalists' self-understanding and the practices of their professional media coverage of the Snowden revelations, which contributed to the normalization of surveillance with an emphasis on national security. Meanwhile, a study of automated artificial intelligence surveillance on the internet and its normalization tendency in the American

community showed that online agreements of sharing information has a normalizing power in a circle of learned behavior from the users' side (Park, 2021). Users perceive data surveillance as a "normal" part of human-machine interaction in digital platforms as another place for social relationships through self-disclosure (Evens & Van Damme, 2016).

As for fear, since 9/11 desire for surveillance measures has been heavily reported in the media. The domestication of security and surveillance in some western countries, such as the US, UK, and Belarus was a momentum crisis resulting in more calls for reinforcement of surveillance, especially, for some marginalized social groups (Astapova, 2017). Thus, technology has been introduced for security purposes and deployed in a sophisticated way to mediate between surveillance and liberty with public service's efficiency enhancement in mind, which undoubtedly, results in more ways of monitoring and collecting personal data.

Contemporary surveillance on social media also could be interpreted as *fun*. For instance, it might have integrated into serious aspects of people's lives such as spare time and entertainment. Surveillance may be "potentially empowering subjectivity and building even playful," stated Albrecht Lund (2008). Similarly, Snowden said in a speech: "I live on the internet" (2015, video).

4.3.2-Users' participatory role:

A key normative aspect of surveillance culture is the imperative to *share*. Deborah Lupton (2014) pointed out that "social media users are enjoying creating content of all kinds and waiting to know others' feedback believing that they have an impact on their networks" (p. 30). Such a crucial power of recirculating and mutual contribution of users, who tried to not be excluded from digital participation via voluntarily sharing among their networks, significantly

affected users' exposure to surveillance (Ball, 2009). Later, Bernard Harcourt (2015) in his book *Exposed* pointed to self-exposure online as a defining feature of these days.

Yet, the user is no longer the subject of such power of involvement in the digital arena but a contributor who competes with the dynamic of social media engagement and an evaluator too (Lyon, 2017). Ball (2009) built on John McGrath's (2004) assumption that users still make a choice, drawing on the meaning and the context of exposure to the subject, whether it may have negative connotations as vulnerability and abandonment or actively sought after for pleasure and satisfaction.

Desire is also an empowering factor for inspiring exposure; it is not only a response to satisfy a need but also a productive force. For Harcourt (2015) social media platforms are encouraging our "self-exposure and self-exhibition." This is particularly seen among teens who believe that unless you are on social media "you do not exist" (Danah Boyd, 2014, p. 5). Boyd underscored that subjects have been numbed by a self-centered thought of themselves and how they were created on social media. Thus, Lyon (2017) concluded that "pleasure and punishment suffuse each other and work together." Meanwhile, Lupton, (2014) exhibited the concept of ethical self-formation on social media in which people configure and represent themselves on it, such as shared life through others' approval or disapproval of one's content by sharing or liking more widely on these platforms. Self-image building or a "self-reflective process" in which participants on social media contribute not only to self-formation but also to social norms and expectations development in different communities.

Hence, social media corporate surveillance is seen as a subjectivity's shaper. Arguably, it is a crucial new development. Harcourt stated that "replenished by our curiosity and pleasure

through retweets, create networks, share, and repost", (p.50), through which they insert surveillance capability into our daily pleasures. The first decade of the 21st century began with harder surveillance introduced by the Department of Homeland Security (DHS), usage of social media in agency security, and demanding social media information of travelers at borders (Gibbs, 2016). Following Harcourt's assumption, desire here is in tandem with another mode of power which is security.

Under the theme of digital network platforms surveillance, they optimize consumers' movements, searching, and purchasing, which is a mix of private and public information. Rather than for security purposes, for Harcourt, it became a post securitarian "expository power" in which all little wants, desires, preferences, beliefs, ambitions, our individuality, and differences shape our digital selves.

4.4-Social media surveillance and beyond:

One more feature of the culture of digital surveillance recalled by Raymond Williams is the reduction of ethical aspects in technical concerns. The cultural concept begets many questions such as how to think, behave, act, and even intervene within varied social imaginaries (Lyon, 2017). Since imaginaries are surveillant, practices should hint at ethical aspects to be performed. For instance, ordinary people need to know how to behave in the digital realm with a prominent level of awareness of multifarious uses and consequences of personal data sharing within the recent digital modernity; from clicking on the shared button, rules of social media platforms, to more sophisticated shared resources and surveillance tactics to be overcome.

Transparency, however, is the main notion of ethics that represents the slogan of the majority of digital corporate communities' standards; "everything that happens must be known",

such a level of transparency has become a “buzzword” of the digital modernity of surveillance capital. To be transparent for such modernity is to be visible to all. Andrea Brighenti (2010) depicted visibility in the social process as a rational process of seeing and being seen that are connected. From his observation of visibility, there is no visible without ways through which seeing is socially and even internationally crafted. Thus, the visible, which represents transparency online, cannot be separated from recognition, its struggles, and politics. Visibility results in the possibility of identification and breeds a culture of identification (Lyon, 2017).

Eric Stoddart, (2012) however, shows another angle of visibility as a more illuminating way of considering surveillance than conventional privacy. Stoddart proposed the in/visibility of managing and negotiating visibility in the social media space. To set an ethical notion for surveillance, care, and self-transcendence. Thus, for Stoddart, “surveillance should not be sole of people, whether technological risk, or privacy isolation, but for people who should practice it carefully and put it in consideration”.

To conclude, the culture of surveillance approach is to analyze the various kinds of imaginaries and practices of surveillance, and to examine their connection with ethical challenges, as well as how users go on in their daily digital life with privacy and data protection, and how they affect social responsibility and citizens.

1. **Conceptual framework: Hypotheses:**

Hypothesis (1) H1: Awareness of social media polices is positively correlated with user's perception of surveillance.

Hypothesis (2) H2: Awareness of social media policies is positively associated with people's concern of privacy and censorship

Hypothesis (3) H3: social media surveillance perception is positively associated with people willingness to share their data

(H3) a: people who perceive surveillance on platforms for commercial reasons are more likely to share their information online.

(H3) b: people who perceive surveillance on platforms for government and security reasons are less likely to share their information online.

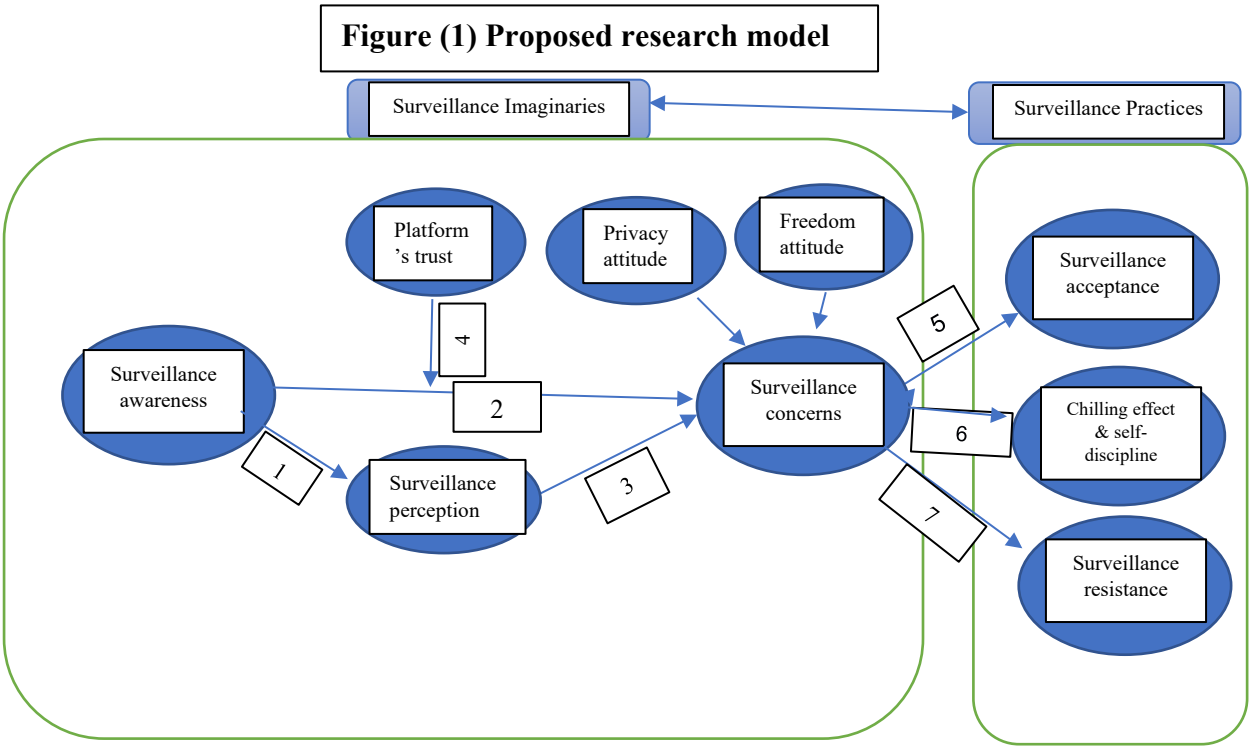
Hypothesis (4) H4: users who trust social media policies are more likely to share their information with these companies

Hypothesis (5) H5: Users' privacy perception on social media platforms is negatively correlated with users' willingness to share data

Hypothesis (6) H6: users freedom perception on social media platforms is positively correlated with self-discipline

Hypothesis (7) H7: Users who are highly concerned surveillance, are more likely to resist or taking neutralization actions on the platforms

Figure 1 :Theoretical framework model



V. Chapter Five:

Methodology:

The study explores the correlation between social media policies' perception as a surveillance tool and its effect on the potential resistance of these policies. Besides, it explores the interaction of multiple approaches of perception and awareness towards people's concerns to be surveilled online and how this will contribute to encountering behaviors against this surveillance. The researcher examined the factors of surveillance culture which were suggested by Lyon (2017). The study is trying to explore the relation between imaginaries of social media policies and practices according to which the users might take action against these policies. Social media policy awareness has been examined in different contexts and its impact has been interpreted through varied theoretical frames, deterrence and chilling effect, and the spiral of silence (Ayaburi & Treku, 2020; Fatima et al., 2019; Wang & Tucker, 2021), yet, to date, none examined the potentiality of user encounter behavior after being aware of surveillance on social media platforms in the Egyptian context.

5.1-Data gathering and sample:

An online survey was conducted to gather data to measure the aforementioned variables. To target social media users, the questionnaire is disseminated during the 2022 spring semester on many social media platforms; Facebook, Twitter, and Instagram; as posts and comments in dozen groups, Messenger, and What's App as private messages. A non-random convenient sample of 547 respondents chose on their own to participate in filling of the online survey. A filtering question was added at the beginning of the survey to limit it only to

Egyptians. This study could be considered exploratory research as it has never examined social media policy resistance before in Egypt. The online form started with a participation consent to affirm the Anonymity of participants and the data gathered will be used for research purposes only. Instead of “surveillance”, “close observation”, “Morakba” in Arabic, is used to avoid misunderstanding of the surveillance as it is not a familiar word to be understood by all. SPSS is used to analyze data, which is one of the most used software in social science. After gathering the data, the researcher coded the variables and examined the correlation between latent variables using Pearson's (bivariate) correlation coefficient.

The first two constructs: Awareness and perception built on John Correia and Deborah suggested a muti- dimensional definition of regulatory of information privacy awareness “as the knowledge of the regulatory elements related to information privacy (IP), the understanding that the elements exist in the environment and projection of their impacts in the future”. In the former definition, they provided an understanding of three type of awareness. For awareness, the knowledge, the researcher use readability as measure of knowledge of the social media policies and terms of consent they should agree on before joining the application. Second, the perception, comprehension of these terms of standard or the consent of the platforms; being able to define reasons of collection information, data and content generated by the users. Further, understand the interrelated relationship between second and third parties regarding individual’s private data. The survey was divided into five sections. Section one is to measure policies awareness based of platforms’ policies readability, to what extent users understand and comprehend information mentioned in the policy agreement, code of standards. Section two devoted to measure policy perception what are reasons of data collection and close monitoring of content generated by users. Privacy and freedom meaning to users on the social media platforms Policy acceptance

and resistance measured in section four. Finally, section five profiled respondents' demographics.

5.2- Measures:

Most of the measurement techniques were developed based on previous studies. Some of the variables were measured using multiple items to achieve a high level of reliability. However, measures were tailored in this study to specifically understand social media users' practices according to certain imaginaries of surveillance policies on these platforms. Imaginaries interpreted into surveillance awareness of the digital platforms' privacy policies, how they perceived their data collected, and to what extent they trusted these platforms. Surveillance practices are interpreted into the behavior users will take as a reaction after being surveilled on the platforms.

Some items were modified to match the scope of the current study. Some variables were examined using the 5-point Likert scale as a measurement of the level of engagement on social media, awareness of its policies, Egyptians' privacy and surveillance attitude, and censorship satisfaction. (5= Strongly agree - 1=Strongly disagree, 5=Extremely confident-1= Extremely unconfident, 5=Extremely concerned- 1= Extremely unconcerned). To ensure scale reliability, Cronbach's alpha is used for all the scales which indicate an above 0, 6 value of internal consistency (Lasinska, 2013).

Table 2: Variables definitions:

Table (2) Variables

Constructs	definition	Author
Awareness	Have a sense of surveillance or read terms of services	Correia &Compeau (2017)
Perception	It is measured according to platforms' statement of data collection purposes For advertising To Promote safety and security To Improve their services	Correia &Compeau (2017)
Trust	To the platforms to fulfill commitment despite the trusting party's dependency and vulnerability	Gefen et al. 2003
Privacy	It is the right to be private from disclosure of the public sphere	(Roberts, 2015b)
Freedom	It is defined as non-interference in speech or in online activities.	(Bennett, 2008)

VI. Chapter Six:

Findings and Results:

6.1- Data analysis:

It is worth mentioning that females represented most of the sample size with 385(70.5%), while males are 161(29.5 %) (Figure 2). The level of education is relatively high 43.7% have a master's degree, 43.4% have a bachelor's degree, 11.7% Ph.D., and 1. has a 3% High School Degree or Equivalent. The respondents' ages ranged from 18 to above 65 years old: 52.5% of the sample were between 25-34 years old, 22.8% were 35- 44 years old, 14.9% were 18-to 24, and 9.3 % were from 45- to 64 and only two respondents are above 64 years old,

Figure 2: Frequency of participants of the Sample according to gender.
Figure 3: Respondents education level

Figure (3)

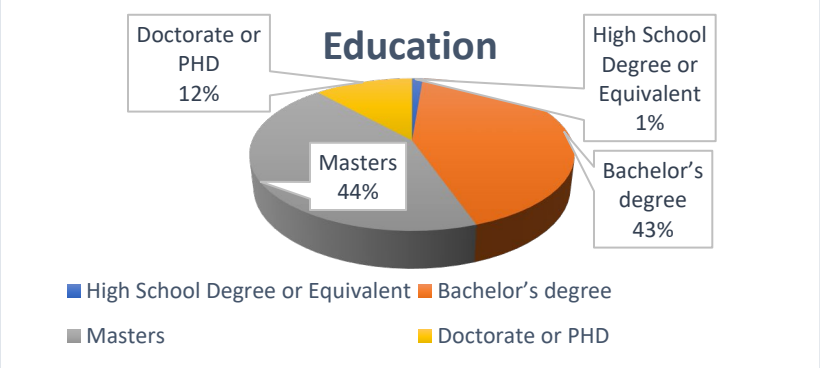
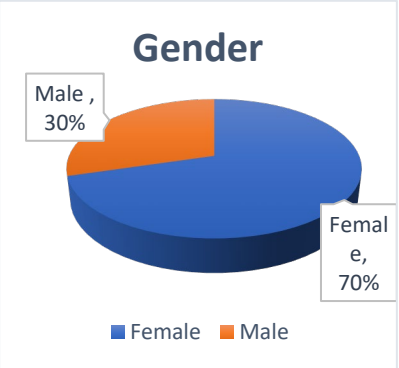


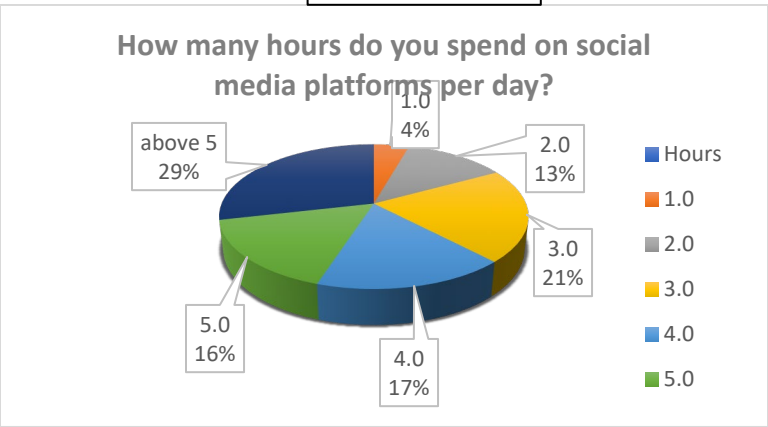
Figure (2)



To make sure that all the respondents are social media users, they asked how many hours they use social media per day. The results showed that 45% spend 5 hours or above on different social media platforms, 38% spend 3 or 4 hours, and only 17% spend one or two hours. [Figure 4]

Figure 4: Frequency of how much time spent on social media platforms.

Figure (4)

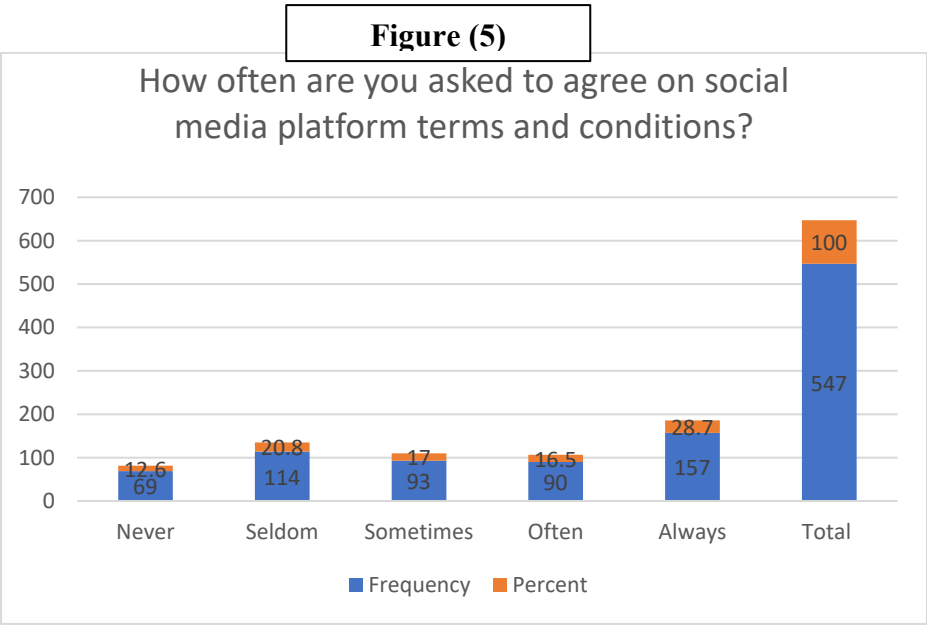


6.1.1-Social media policies awareness:

The items used to measure the variable "*surveillance awareness*" adopted from some platforms' consent. The respondents were asked whether they are reading these consents before agreeing on it, the amount of information collected from them, and how much they feel they understand social media community standards.

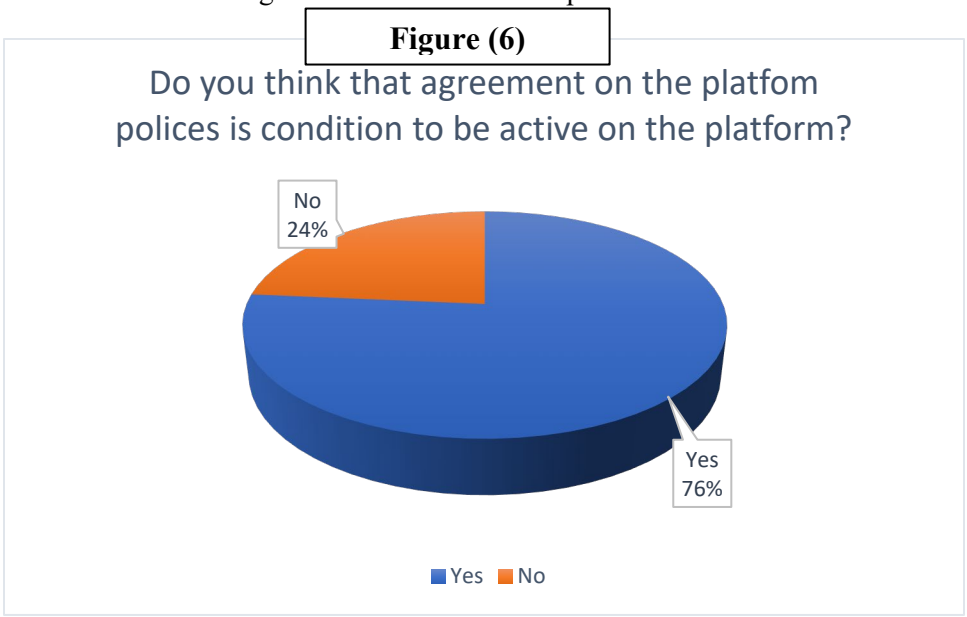
Almost 28. 7 % of the participants said they were "always" asked to agree to the platform's terms and conditions before joining the platforms, while 16.5% are "often" whereas 17 % almost do not know if they are asked before joining or not. Whereas 33% of the participants "rarely" have been asked or even never been asked before. [Figure 5]

Figure 5: Frequency of term of condition agreement on social media platforms



When people were asked if the agreement on platform policies a condition is to be a platform's user, 76% said yes, however, 24% think they can be a user without agreeing on the term of condition. [Figure 6]

Figure 6: Conditions of terms of agreement on social media platforms.



The figure – shows that most of the sample "rarely" or "never" read platforms' terms or conditions before agreeing on them, while only 8.2% (45 respondents) "always" read the code of standard of the platforms. The mean of the possibility of reading the policies is 2.34 with SD=1.283. [Figure 7]

Figure 7: Frequency of term of condition possibility of reading

Figure (7)

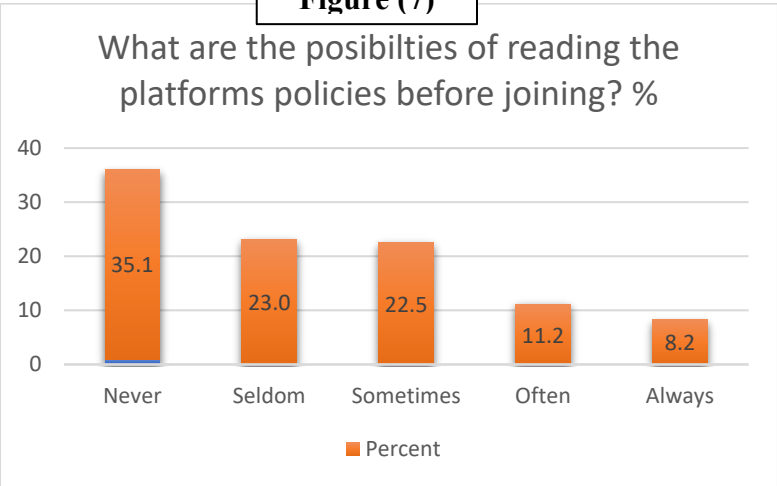


Table 3: Frequencies of term of conditions readability

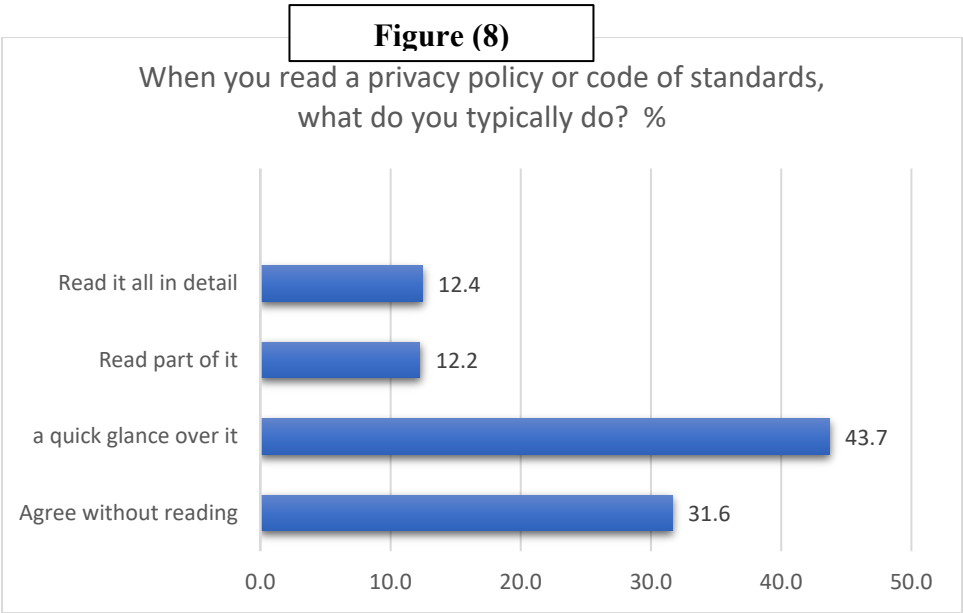
Table (3)

what are the possibilities of reading the platform's policies before joining?

N	Valid	547
	Missing	0
Mean		2.34
SD		1.283

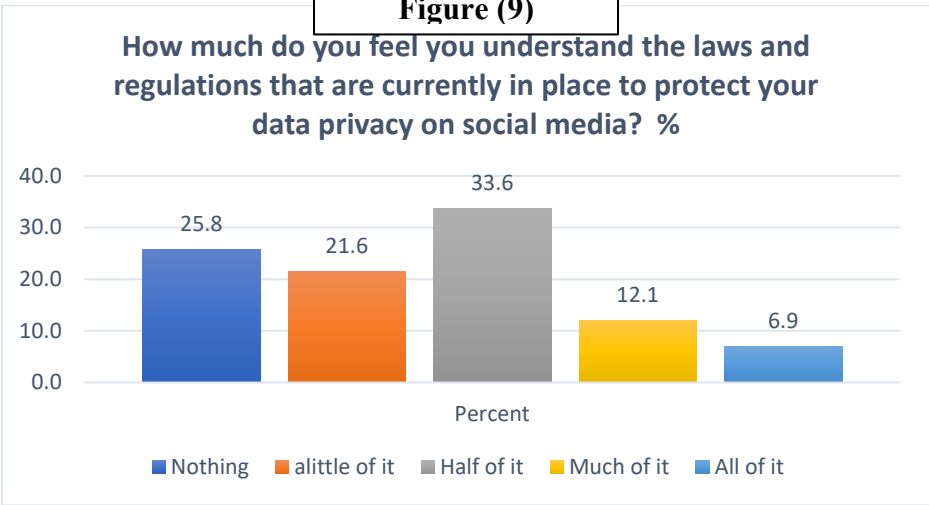
Yet, among the respondents who read the platforms only 12.4 % (68 participants) read it in detail, and 12.2 % read part of it, while the majority 43.7% have a glanced over it, but the third (31.6%) of the sample agree without reading. [Figure 8]

Figure 8: Frequencies of different four technique of policies reading.



The participants were asked how much they understand platforms terms and policies, 25.8% understand “nothing of policies polices, 21.6 % understand a little of it, one-third third of the respondents said they understand half of the policies. Whereas 12.1 and 6.9 understand much of it and all of it respectively. [Figure 9]

Figure 9: The percentages of policies comprehension to the respondents



The results show that respondents believe a high amount of their information is tracked by social media platforms; 37% think 91-100 % of their information is tracked, 31% choose 71-90, and around 14% think that from 50 – 70 % of their data is tracked. Only 8% choose from 31-50 % of their data is tracked whereas only 6% said that less than 30 of their data is tracked.

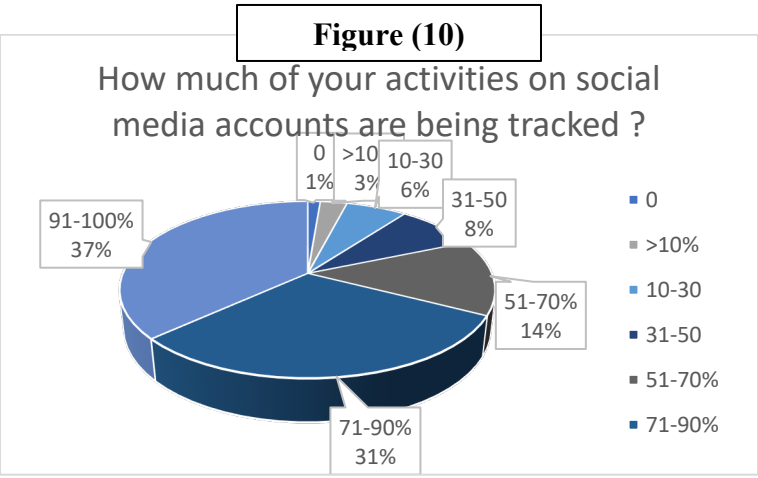
The mean of the data tracked is relatively high (M= 4.32, SD=1.045) which indicates that the sample is aware that there is a high amount of their data tracked by social media platforms. [Figure 10].

Table 4: the means of policy readability

Table (4)

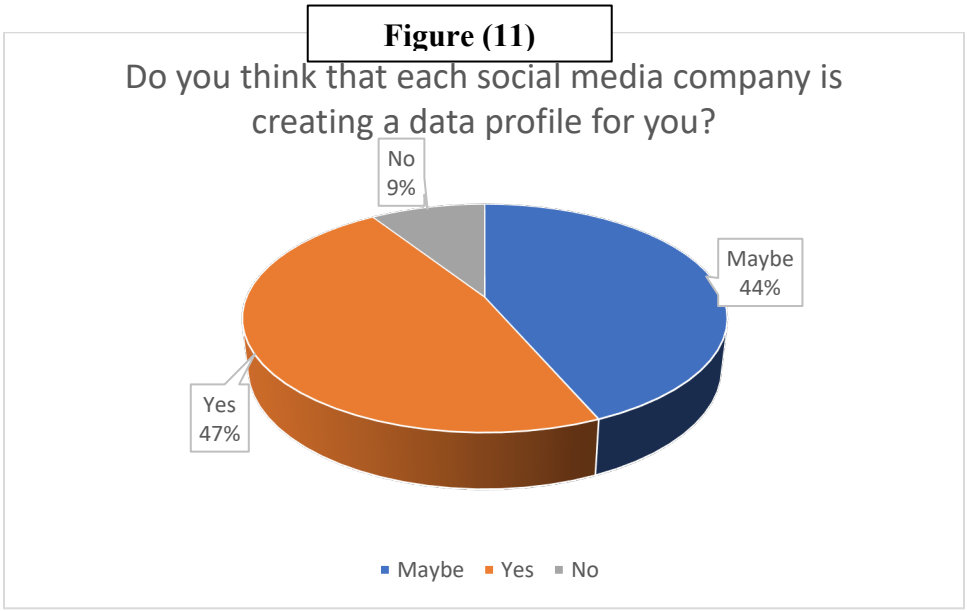
	N	Minimum	Maximum	Mean	Std. Deviation
How much of your data is tracked by social media companies?	547	1	5	4.32	1.045

Figure 10: The percentages of the amount of data tracked on social media platforms



The respondents were asked if they think that each social media platform creates a profile for them. Around the half (47%) of them said “yes”, the platforms create a profile for them and the other 44% of the participants think that “maybe” there is a profile for them on platforms whereas only 9% (only 51 of the respondents choose “no”). [Figure11]

Figure 11: The frequency of respondents who think that companies create a profile for each user



6.1.2-Public perception of social media policies regarding data privacy:

The perception of social media platforms' policies over the data is measured through different constructs. To highlight if it is for the platforms, government, or the users. "To increase platforms' profits" is chosen by most of the respondents as the main goal of the platforms 78.2 % choose "yes" rather than "no" or "maybe". "To help the government" is the second goal for collecting user-user for 63.4 %of respondents. While the selection of "to help users" is the last option for the participants in this sample 41%. [Figure 12]

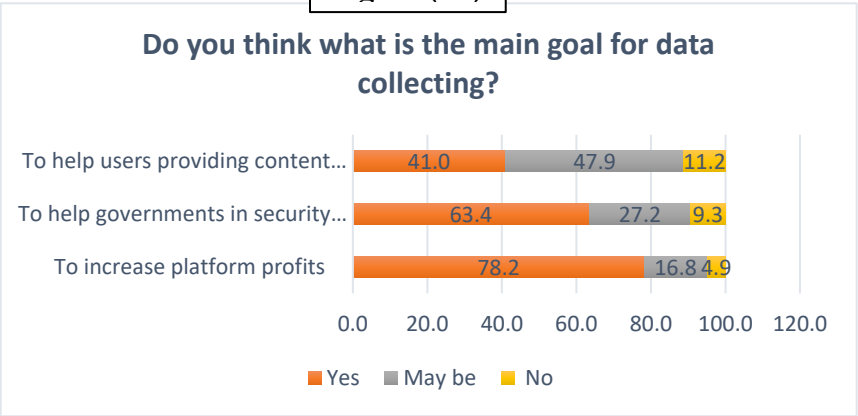
Table 5: Policy perception means

Table(5)

Policy perception	Means	SD
To increase platform profits	1.27	.543
To help governments for security reasons	1.70	.658
To help in providing content users need easily	1.46	.660

Figure 12: The frequency of data collection reason

Figure (12)



When they were asked to what extent they are concerned or worried about the data collected the majority chose “neutral” 32 % were neither concerned nor unconcerned about their data. While 25.6 are moderately concerned and 22.9 % are extremely concerned. Whereas only 12.4 % are slightly concerned or worried about their data, and 7.1% are not worried at all about their data. [Figure 13]. Social media users concerned have a mean of 3.45 with SD=1.176.

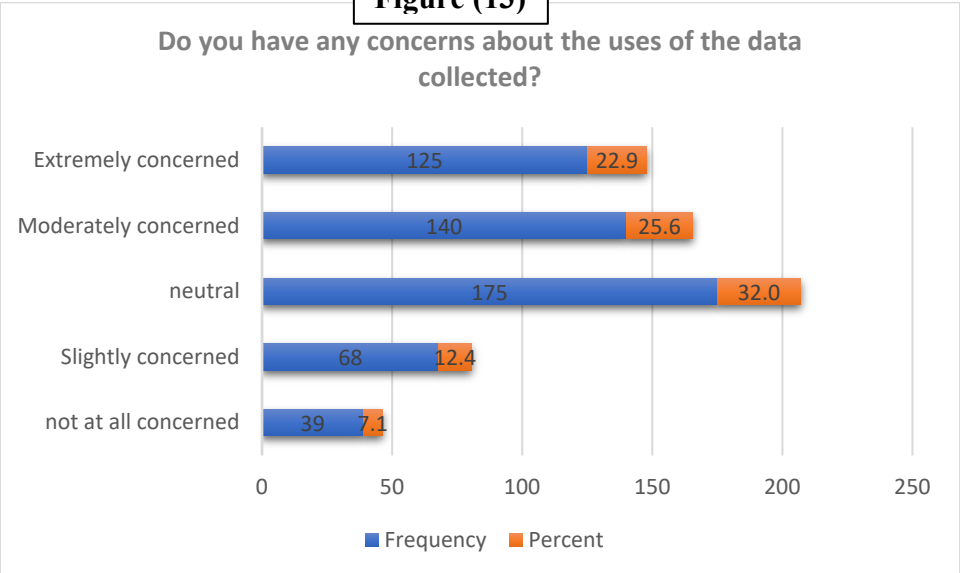
Table 6: The means of concerns of data collection.

Table (6)

	N	Minimum	Maximum	Mean	Std. Deviation
Do you have any concerns about the uses of data collected	547	1	5	3.45	1.176

Figure 13: The frequency of concerns of data collection

Figure (13)



The result shows that to some extent users do not benefit from data collected from their accounts on the social media 26% and 25.2% of the sample select “nothing” and “a little” respectively of the data is beneficial for them, whereas 30.5 select “somewhat” of the data. Only 13.2 and 4.9% selected “much of it and a Great deal of it “respectively as data collection is beneficial for them on the platforms, [Figure 14]. The mean of these items was 2.46 with SD= 1.153, indicating the fewer benefits users get from the data processing.

Figure 14: The frequency of personal benefits of data collection

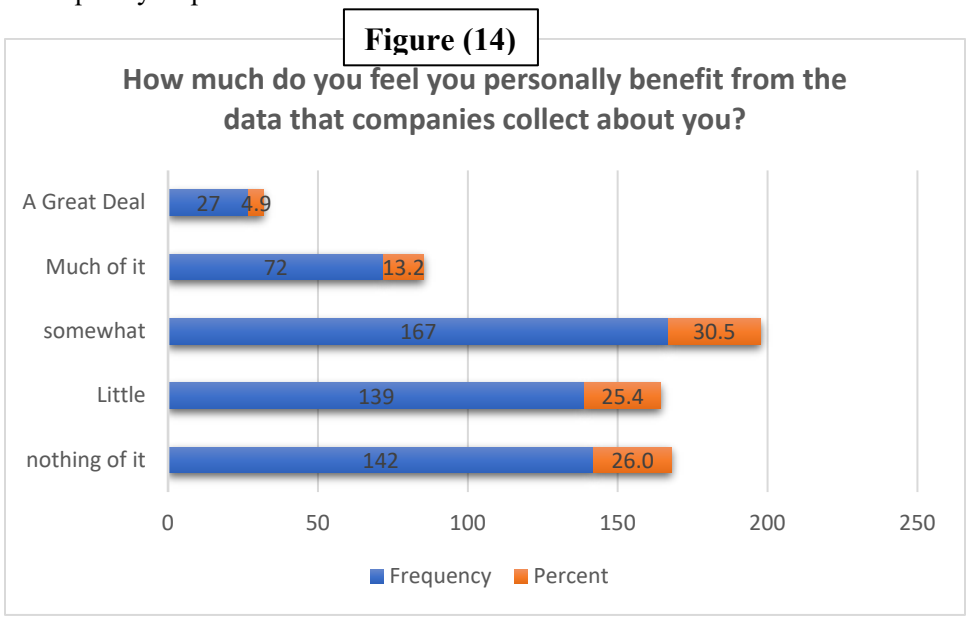


Table 7: The means of data collection risks.

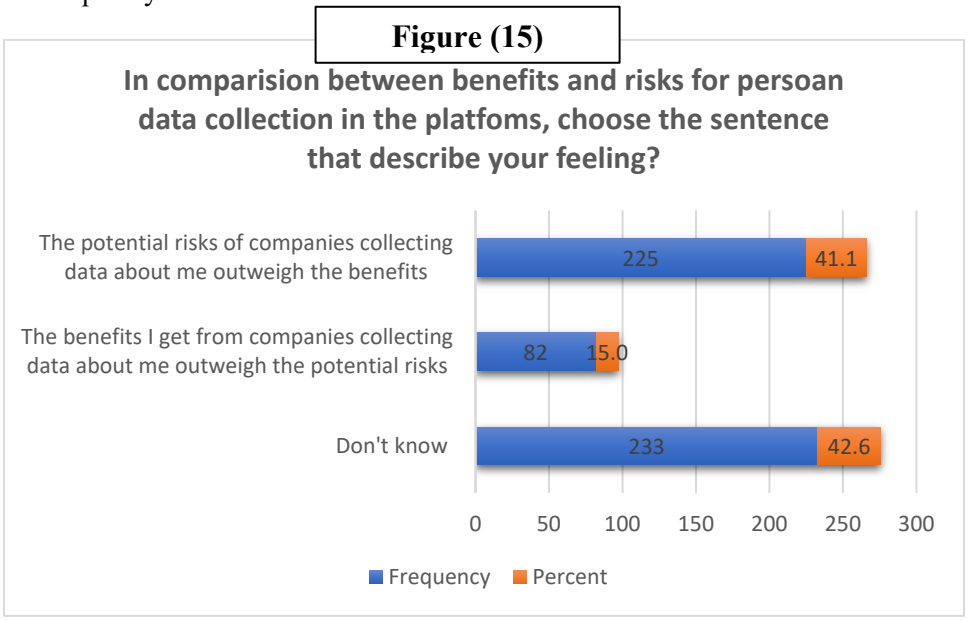
Table (7)

	N	Minimum	Maximum	Mean	Std. Deviation

How much do you think you benefit from data collected from your account on social media platforms?	547	1	5	2.46	1.153

In a comparison between the benefits and risks around 41.1 % of the sample selected that the potential risks outweigh the benefits. On other hand, only 15 % selected that the benefits they get from collecting their data outweigh the risk. Around 42.6 do not know if data is benefiting them or putting them at risk. [Figure 15]

Figure 15: The frequency of risk of data collection



6.1.3-Accept sharing information: (α=0.773)

Since sharing data with platforms is still a choice for social media users, the respondents are asked for the purposes they are more comfortable sharing their data for; "to help them in the content they need: 9.7 % and 41.7 strongly agree and agree respectively to share. Around 30.5% are neural in sharing data for the mentioned purpose whereas only 6.2 % and 11.9 disagree and strongly disagree share data for the same purpose respectively. The mean for this item is the highest among the rothers purposes in the next paragraph, (M=3.31, SD= 1.117).

Moreover, people are comfortable sharing their information to prevent crimes on these platforms. Around 8% and 38.2 "strongly agree" and "agree" respectively to "to improve fraud prevention on the platforms", and 32.5 are "neutral" for sharing data for this purpose. On the other hand, only 7.5 % disagree with sharing their data to prevent crimes on social media platforms, and 13.7 "strongly disagree" with this. The means for this item is the second for comfortability to share information for certain purposes, (M=3.19, SD= 1.137). "To adjust users' behaviors" is in the middle among the 5 items, (M=2. 92, SD= 1.208), 7.3 and 29.2 strongly agreed and agreed respectively on this item while 29.4% are neutral regarding this item. However, around 16.1% and 17.9 disagree and strongly disagree respectively. "To help the government in security measures" is strongly disagreed and disagreed by 30.5% and 15.9 % respectively, whereas agreed and strongly agreed by 17.9 and 5.7 % respectively. (M=2.52, SD=1.250). "To increase engagement and advertising" mostly disagreed with the respondents; 32.5 % and 21.6% strongly disagree and disagree, 25.2 %are neutral and 16.5% and 4.2 % agree and strongly agree. (M=2.38, SD 1.213). [Figure 16]

Figure 16: the frequency of people comfortability sharing their information

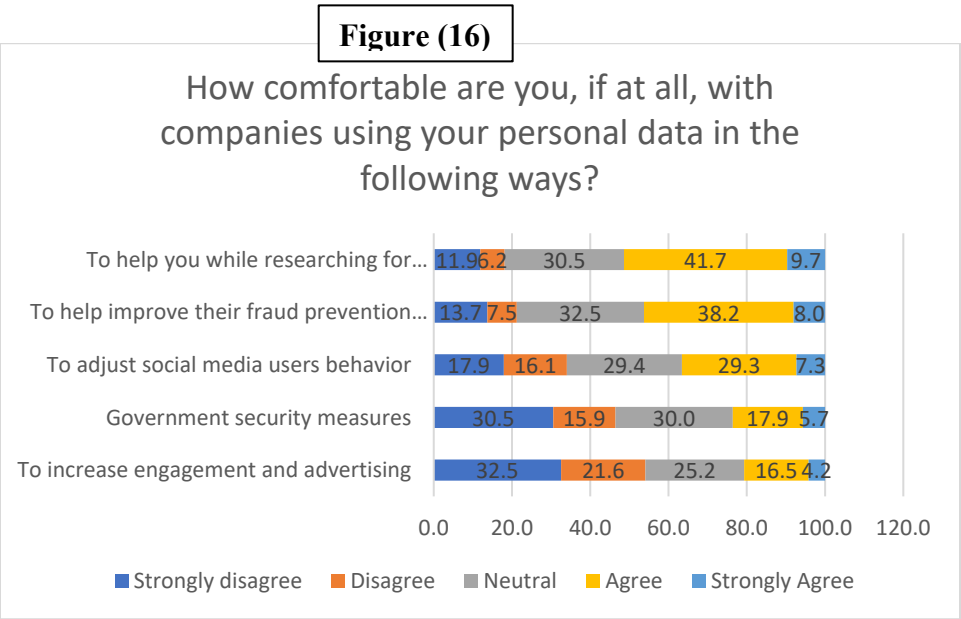


Table 8: The means of data collection benefits

Table (8)

How comfortable are you with companies using your data in the following ways?	N	Minimum	Maximum	Mean	Std. Deviation
To increase engagement and advertising	547	1	5	2.38	1.213
To help improve their fraud prevention systems	547	1	5	3.19	1.137

To adjust social media users' behavior	547	1	5	2.92	1.208
To help Government with security measures	547	1	5	2.52	1.250
To help you while researching something	547	1	5	3.31	1.117

6.1.4-Users trust the social media companies: (α=0.728)

The purpose of the next question is to highlight the amount of users' trust in social media platforms which can affect their willingness to share their data. The items used to measure to what extent users trust social media companies showed that users are "not confident at all" in the companies to "publicity admit mistakes and take responsibility of data misuse" by 44.6 %, while slightly not confident by 25.8%. This item scored mean is 1.99 with SD= 1.101.

Similarly, the "Be held accountable by government" item, (with a mean of 2.06 and SD= 1.107), recorded 41.5 % not confident at all and 24.5 % slightly not confident. To be notified by the company if it misuses your data recorded 37.1 % "not confident at all" and 26 "slightly not confident". The mean for this item is 2.21 with SD=1.186.

Likewise, the respondents suspect that the companies will follow privacy policies. Around 20.1 % are "not confident at all" and 34.2 % select "slightly not confident". (M= 2.41 with SD=1.022). (Figure 17]

Figure 17: The frequency of people confident in companies

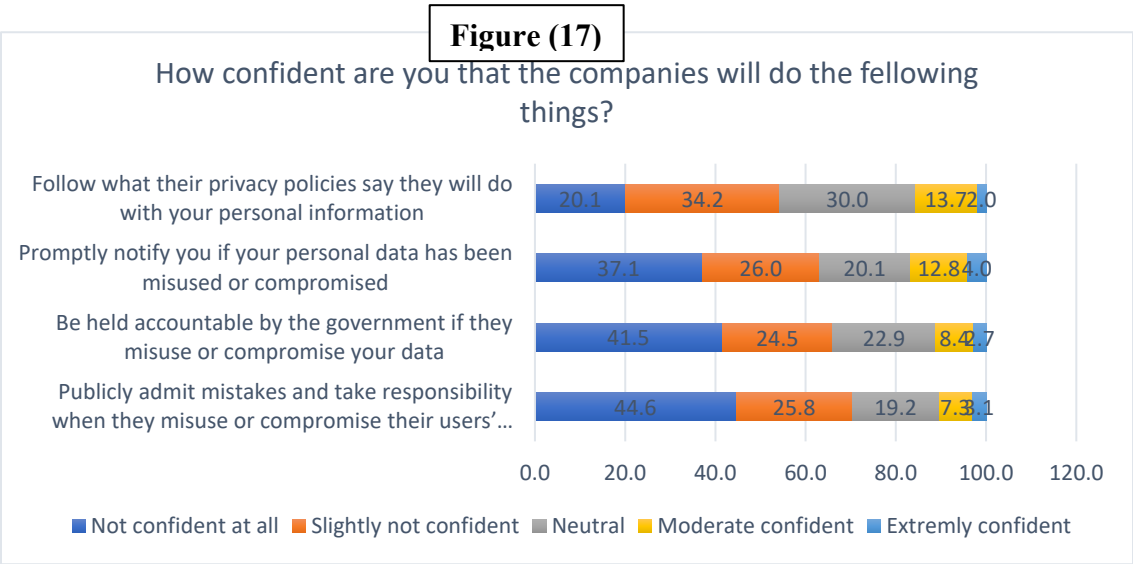


Table 9: The means for sharing data comfortability

Table (9)

How confident are you that companies will do the following things?	N	Minimum	Maximum	Mean	Std. Deviation
Follow what their privacy policies say they will do with your personal information	547	1	5	2.43	1.022

Promptly notify you if your data has been misused or compromised	547	1	5	2.21	1.186
Publicly admit mistakes and take responsibility when they misuse or compromise their users' data	547	1	5	1.99	1.101
Be held accountable by the government if they misuse or compromise your data	547	1	5	2.06	1.107

6.1.5-Social media users' surveillance attitudes: (α=0.883)

A construct to examine the "data privacy attitude" of Egyptian users show that people are highly concerned about their privacy. For respondents "not being monitored at social media platforms" and "not being watched or listened to by anyone or a machine" identically are selected by 32% of the whole sample as extremely important items. The means for both items are (M=3.5, SD= 1.333) and (M=3.58, SD=1.123) respectively. Likewise, items "Being able to share confidential information with friends through the platform ", "being out of social media surveillance and

algorithms influence", "To share information anonymously with advertisers" and "control over the type of information to be shared with social media platforms" chosen by 29.3%, 26.1%, 25 %, and 21.8 % respectively, as the most important in regard their data privacy. [Figure 18]

(M=3.37, SD= 1.385), (M=3.37, SD=1, 294), (M= 3.23, SD= 1.222) and (M=3.27, SD=1.280)

Figure 18: The frequency of privacy meaning for users

Figure (18)

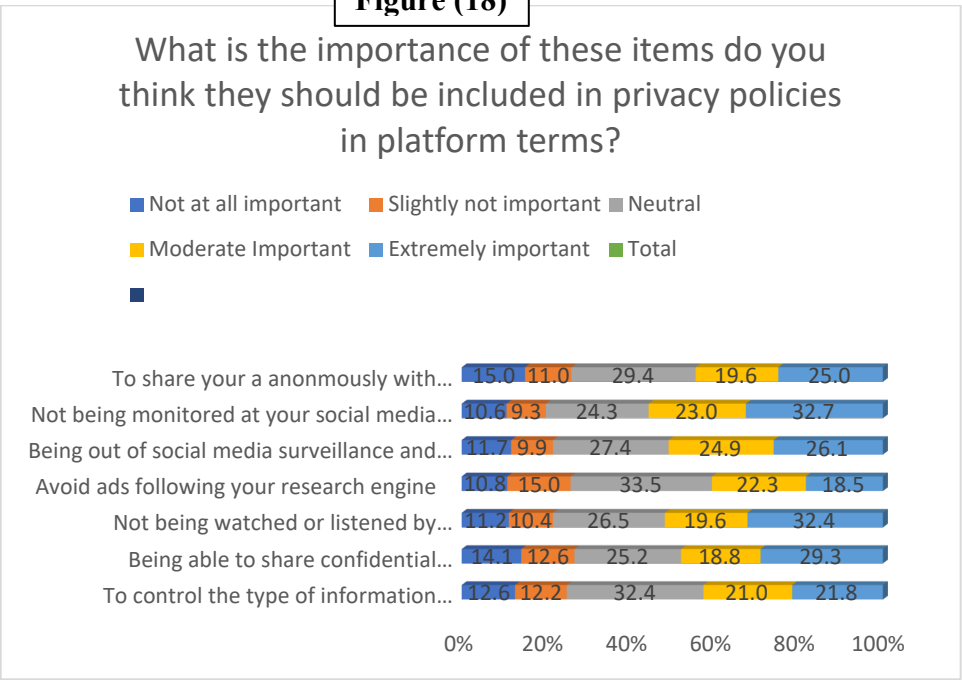


Table 10: the mean of frequency of people confident in companies.

Table (10)

What is the importance of these items do you think they should be included in privacy policies in platform terms?	N	Minimum	Maximum	Mean	Std. Deviation
To control the type of information platform collected from your account	547	1	5	3.27	1.280
Not be watched or listened to by someone or a machine without your permission	547	1	5	3.52	1.333
To use your information anonymously	547	1	5	3.23	1.222
Not receiving ads following your research engine	547	1	5	3.44	1.293

To be out of social media platforms monitoring	547	1	5	3.58	1.313

6.1.6-Social media users' freedom polices attitude: (α=.872)

Users' attitude toward their freedom on social media platforms is important to most of the respondents. The freedom attitude was measured using five items. The means and SD of all items are consistent with each other. The first item is "being in control over what kind of information could be shared with social media platforms" M=3.68, SD= 1.270. The second item "being able to share content without platform intervening in your words or point of view" means equal to 3.63 and SD equal to 1.216. The third item, "No one or machines watch or listen to you without your permission, (M= 3.19, SD= 1.239). Items fourth and fifth means (M= 3.33, SD=1.261) and (M=3.46, SD=1.279).

Table 11: The means of privacy meaning for users

Table (11)

Users' freedom of importance on social media	N	Minimum	Maximum	Mean	Std. Deviation

Being in control over what kind of information could be shared with social media platforms	547	1	5	3.68	1.270
Being able to share content without the platform intervening in your words or point of view	547	1	5	3.73	1.216
No one or a machine watch or listens to you without your permission	547	1	5	3.91	1.239
Not being disturbed by warnings, flagging, or spam from the social media platform	547	1	5	3.33	1.261
No revision to any content on your account	547	1	5	3.46	1.279

To explore if the respondents have ever experienced any policy violation before on social media platforms, a question was asked to them “have you ever been notified of a policy violation before?” The most of respondents have not violated any social media policies before 55.2 % while 44.8 %have been notified of policy violations. (Figure --). However, around 38.9 % of how to have been notified are “extremely not satisfied “measure the platforms detected their policies over them. While 14% are slightly not satisfied with the measure taken against their violation and 28% (70 respondents) were neither satisfied nor dissatisfied regarding the measure. Whereas only 12% (30 respondents) and 5% (13 respondents) are extremely satisfied with the measures taken against their policy violation. The mean scored 2.31, SD=1.255. [Figure 19]

Figure 19: The number of participants experienced policy violating

Figure (19)

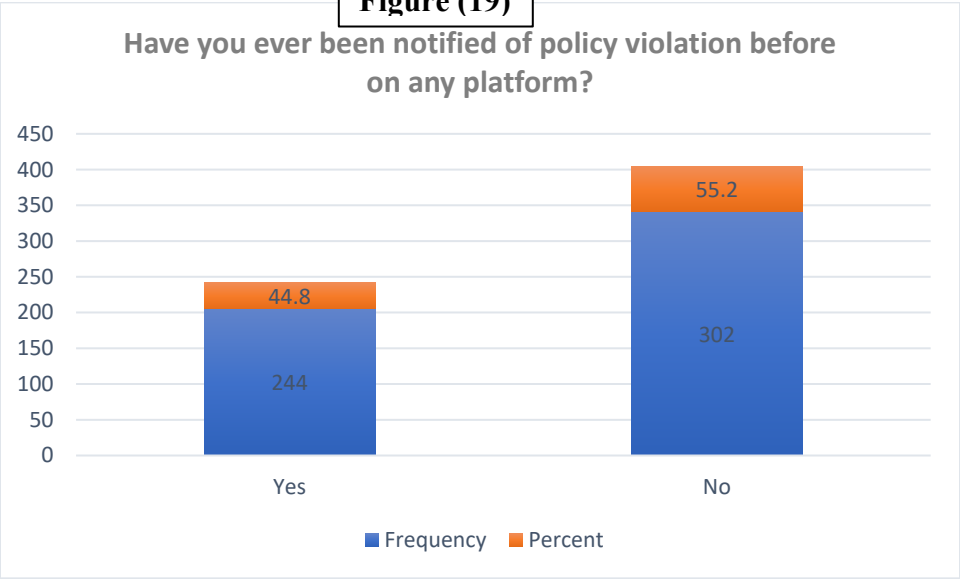


Figure 20: The frequency of respondent's satisfaction

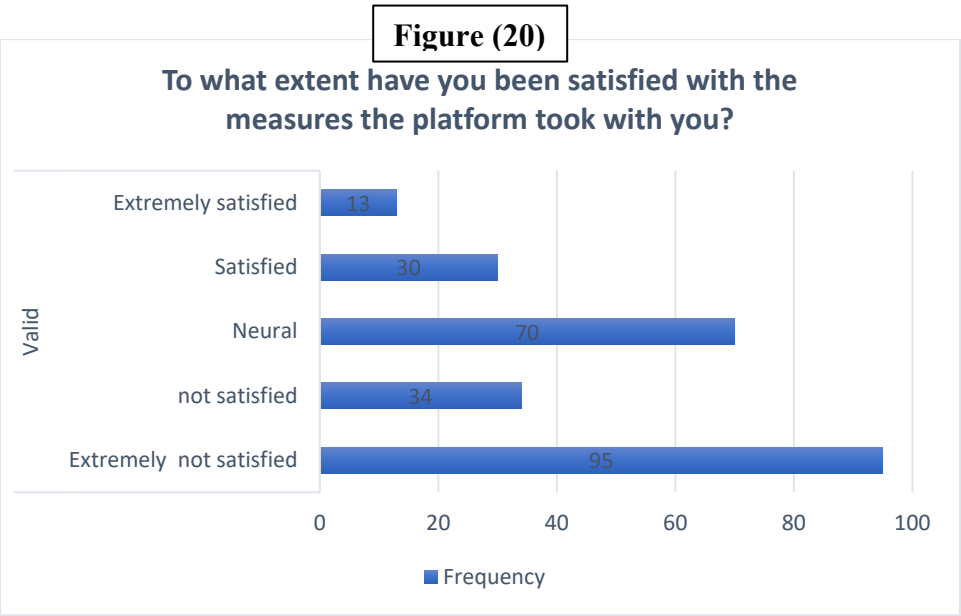


Table 12: The means of freedom meaning for users

Table (12)

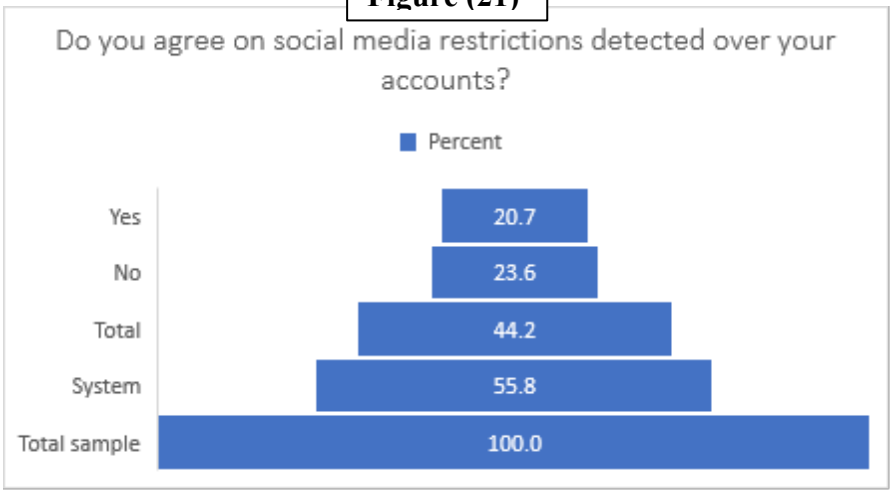
	N	Minimum	Maximum	Mean	Std. Deviation
To what extent have you been satisfied with the measures the platform took with you?	242	1	5	2.31	1.255

The diagram below shows how many respondents refuse social media restrictions over users. Out of the 44.2 % who have been notified of policy violations on platforms, around 23.6 % are

against these restrictions and measures detected over them whereas 20.7 % select “yes” to be restricted by social media policies. [Figure 20]

Figure 21: The number of respondents who against social media restrictions

Figure (21)

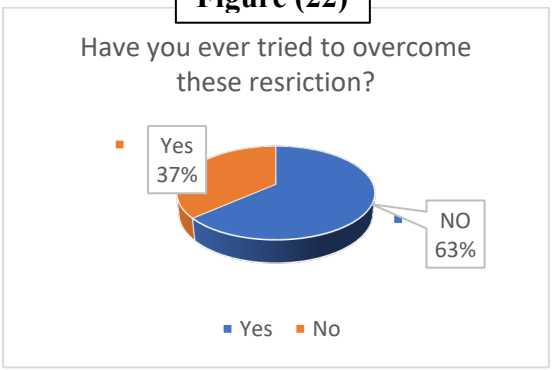


6.1.7-Social media policy resistance:

The potential resistance construct was examined by asking respondents if they have ever tried to resist social media platforms’ surveillance before or not. Around 155 respondents selected “No” (63.5%) and 89 (36.5%) selected “Yes”. (M= 1.28, SD= .449) [Figure 22]

Figure 22: The number of respondents who tried or would like to overcome restriction

Figure (22)



The possibility of resistance was measured with multiple items, based on a literature review. Each item was measuring the extent to (yes, no, maybe) to which the respondents take certain action against social media surveillance. In addition, some items were added to measure if respondents will prefer policy restricted, being self-discipline respondents. "Chilling effect" which refers to self-discipline, is measured through three items "Follow platforms restriction to avoid warnings and notifications", (M=1.9, SD=.834), "Review and adjust my content to fit platforms policies" (M= 1.93, SD=.930) and "Avoid sharing personal data on the platforms" (M=1.54, SD=.763). Surveillance resistance potential was measured by seven items "Disabled location setting for the platform" (M=1.59, SD=.763), "Disabled camera access for the platform", (M=1.54, SD.817), "Use slang language or Franco Arabic" (M=1.88, SD=.905), "Decrease the app rate on the app store", (M= 1.9, SD=.940). [Figure 22]

Table 13**: The means of potential resisitant**

Table (13)

Chilling effect	Average	Mean	St. D
Follow platforms restriction to avoid warnings and notifications	1-3	1.9	.834
Review and adjust my content to fit platform policies	1-3	1.93	.930
Avoid sharing personal data on the platform	1-3	1.54	.763
Surveillance Resistance (Neutralization techniques)			
Disabled location setting for the platform	1-3	1.59	.816
Disabled camera access for the platform	1-3	1.54	.817

Use slang language or Franco Arabic (Write Arabic in English letters)	1-3	1.88	.905
Decrease the app rate on the app store	1-3	1.9	.914
Use memes, or photos, and sarcasm	1-3	2.4	.861
Switch to a different platform	1-3	2.1	.826
Stop using the app	1-3	2.19	.845

Figure 23: Show the respondent's response on how they might avoid social media control

Figure (23)

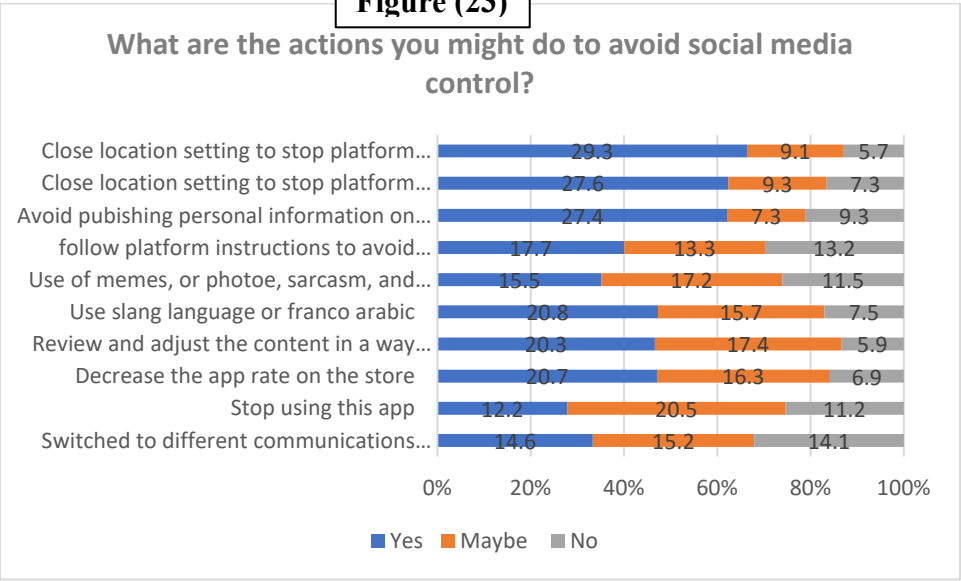


Table 14: Variables scales reliability

Scales Reliability Statistics

Table (14)

Scale	Cronbach's Alpha Based on Standardized Items	N of Items
Users' trust in the social media platforms	.728	4
How comfortable are you, if at all, with companies using your data in the following ways?	.773	5
Privacy is important to social media users	.883	7
Freedom of importance on social media platforms for its users	.872	5

6.2-Hypotheses testing:

Hypothesis (1): Awareness of social media polices is negatively correlated with user's perception of surveillance, Table (15)

Correlations between policies awareness and policies perception

Table 15: Correlations between policies awareness and policies perception

Table (15)		Q1101	Q2201
Surveillance awareness	Pearson Correlation	1	-.017
	Sig. (2-tailed)		.694
	N	547	547
Surveillance perception	Pearson Correlation	-.017	1
	Sig. (2-tailed)	.694	
	N	547	547

The researcher hypothesized that surveillance awareness is associated with users' perception of surveillance. The results show a weak negative correlation between awareness and perception. Pearson's r (547) =. -.017. This correlation is insignificant p= .694, (p>.05). However, people do not read social media policies and do not understand most of it, they can guess for what purposes their data users for what purposes.

Hypothesis (2): Awareness of social media polices is positively associated with people's concern of privacy and censorship (surveillance).

Table 16: Correlations between policies' awareness and user's concerns

Table (16)		Q110 1	Social media user's concerns
Surveillance awareness	Pearson Correlation	1	.095*
	Sig. (2-tailed)		.027
	N	547	547
Social media users' policies concerns	Pearson Correlation	.095*	1
	Sig. (2-tailed)	.027	
	N	547	547

*. Correlation is significant at the 0.05 level (2-tailed).

In this hypothesis Table (16), the researcher intended to examine the correlation between surveillance awareness and users' concerns about their data and personal information on social media platforms. A Pearson's r data revealed a strong positive correlation since r (547) =.095*

However, p showed that the correlation is highly significant (P=.027) which means that p<0.05.

Hypothesis (3): social media surveillance perception is positively associated with people willingness to share their data

(H3) a: people who perceive surveillance on platforms for commercial reasons are more likely to share their information online.
(H3) b: people who perceive surveillance on platforms for government and security reasons are less likely to share their information online. Tables (17)

Table 17: ANOVA test result between social media surveillance perception and willingness to share data

Table (17)

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
To increase platform profits	Between Groups	1.246	4	.312	1.057	.377
	Within Groups	159.785	542	.295		
	Total	161.031	546			
To help governments for security reasons	Between Groups	1.685	4	.421	.972	.422
	Within Groups	234.743	542	.433		
	Total	236.428	546			
To help in searching and providing content you need easily	Between Groups	3.513	4	.878	2.031	.089
	Within Groups	234.312	542	.432		

	Total	237.824	546			

To examine if there is a relation between users' surveillance perception and their concerns about data. A t-Test result showed a statistically insignificant relationship between people's perceptions and concerns. However, users who perceive data social media surveillance to help platforms to increase their profits reported a higher level of concern than found with the assumption that data surveillance for proving user's content needs and for helping governments in security measures.

Hypothesis (4): users who trust social media policies are more likely to share their information with these companies. Table (18)

Table 18**:** Correlation between users 'trust and willingness to share

Table (18)

Correlations

		Q3304	Q3305
Users' trust in social media companies	Pearson Correlation	1	.255**
	Sig. (2-tailed)		.000
	N	547	547
Willingness to share their data	Pearson Correlation	.255**	1
	Sig. (2-tailed)	.000	
	N	547	547

**. Correlation is significant at the 0.01 level (2-tailed).

The researcher hypothesized, based on literature, the correlation between users' trust in social media companies' policies and willingness to share their data with these companies. The above table shows a weak positive correlation between two variables, r (547) = .255**; however, it is statistically significant, p=.001, p<.05.

Hypothesis (5): Users' privacy perception on social media platforms is negatively correlated with users' willingness to share data. Table(19).

Table 19: correlation between users' perception to privacy policies and willingness to share

Table (19)

Correlations

		Q4401	Q3305
Users' perception privacy policies	Pearson Correlation	1	-.161**
	Sig. (2-tailed)		.000
	N	547	547
Willingness to share data	Pearson Correlation	-.161**	1
	Sig. (2-tailed)	.000	
	N	547	547

**. Correlation is significant at the 0.01 level (2-tailed).

The results above indicate a statistical significate relation (p=0.001) between privacy perception on social media and users' intention to publicity share their information with these platforms; however, this correlation is a weak negative correlation r (547) = -.161**

Hypothesis (6): User's freedom perception on social media platforms is correlated with self-discipline.

Table 20: correlation between User perception of freedom on social and users' self-discipline on these platforms

Table (20)

Correlations

		Q55044	Q4402
User perception of freedom on social media platform	Pearson Correlation	1	-.177**
	Sig. (2-tailed)		.006
	N	242	242
Users' self-discipline on these platforms	Pearson Correlation	-.177**	1
	Sig. (2-tailed)	.006	
	N	242	547

**. Correlation is significant at the 0.01 level (2-tailed).

Users 'views of freedom on social media platforms are relatively correlated with their self-control over their activities on these platforms. Yet, such a relation is statistically significant (p =.001), it is a weak negative correlation between the two variables. r (547) = -.177**

Hypothesis (7) H7: users' surveillance concerns on social media platforms are correlated with the intention to resist social media surveillance.

The test demonstrated that there is no relationship between privacy perception and users intention to resist social media policies or surveillance online, however, users who think that social media is a place to share freely their content without platform interference are more likely to resist social media platform restrictions.

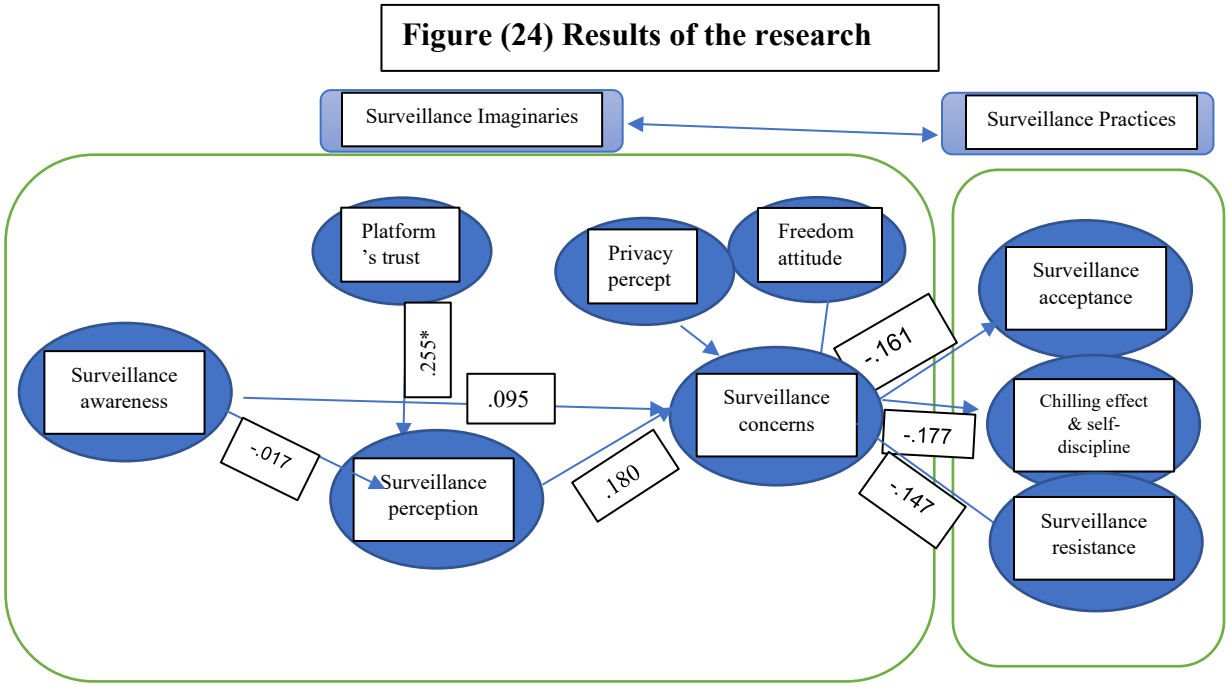
Table 21: ANOVA Test result between privacy perception and Freedom perception

Table (21)

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Privacy perception	Between Groups	20.832	16	1.302	1.362	.162
	Within Groups	215.129	225	.956		
	Total	235.961	241			
Freedom perception	Between Groups	22.141	16	1.384	1.693	.049
	Within Groups	183.906	225	.817		
	Total	206.047	241			

Figure 24: Research model results



VII. Chapter Seven:

Discussion and Conclusion:

This study highlighted important determinants of social media surveillance policies. Specifically, the present study attempts to understand social media users' behaviors based on their level of awareness of surveillance, which means an awareness of policies states on platforms terms of services and privacy policies and regulation of these mediums. In addition, the study analyzes and defines users' perceptions of these regulations and their impressions of these policies.

This study utilized the surveillance culture interdisciplinary theoretical approach as a proposed model to identify the interrelated relationship between policy imaginaries and user practice. Accordingly, practices are users' behaviors that fall into three different categories: acceptance of these policies and following the regulations with open access to their own data, chilling effect or self-discipline by inhibiting legitimate behaviors such as sharing one's opinion online. Finally, resistance to these policies and regulations to neutralize policies' effect on accounts, whether for data collection or close observation of their activities online. Understanding the cognitive processes by which social media users arrive at certain attitude toward online surveillance is important from different cultural perspectives.

The study is also an attempt to highlight the participatory role of social media users in negotiating or resisting contemporary social media surveillance as an end user. This includes determining the meaning of surveillance for users and how their perceptions may impact their behavior on/towards social platforms. The findings showed that users are able to address surveillance online; however, they may be unaware of all social media platforms tools used for surveillance. Ultimately, users perceive surveillance differently; however, the majority assume it

is more for commercial purposes rather than for security or even for users themselves. Although the majority of the sample have never experienced any kind of policy violation on these platforms, a proportion of the sample are highly concerned about social media‘s monitoring of their activities online. Thus, users might not fully understand surveillance because they have not read the policies nor experienced it before.

Conversely, users with a high level of awareness of surveillance or have previously have experience policy violations are more likely to employ self-controlling or self-inhibiting behaviors rather than resisting these policies. These users tend to decrease their social media engagement rather than control the platform’s options. The surveillance culture is a normalized as non-resistible phenomenon for high proportion of the research sample. Thus, the concept of the participatory role of users as an agent who is able to counter social media surveillance is not yet clear. Surveillance definition as well as its effects are shaped by heterogeneous actors who are aligned to shape it. Thus, it is not an easy to be defined into one context or culture.

The results did not demonstrate a relationship between surveillance awareness and surveillance perception. Although people do not tend to read policies in detail (Terms of Services) as suggested in the literature review, they assume that all their activities online are monitored by these platforms. Interestingly, the find ings showed that a high number of respondents presume that more than 70% of their data is tracked by these companies; this could be explained by the high number of similarities they find on their news feeds and notifications suggesting connections and products. The majority of those surveyed answered that they do not fully understanding the policies and regulations, indicating that participants do not know that a profile of their data is created for each user to be targeted according to his/her preferences. This is consistent with prior studies (Jeong & Kim, 2017), which delineated that most social media

users had never read the terms of services or policies and regulations and find the language of these policies not easy for ordinary users to understand.

On the other hand, there is a strong correlation between users' awareness and concern regarding surveillance on social platforms. People with a high level of awareness of policies and regulations are strongly concerned about being tracked and monitored. Due to the information leaks and opaque social media practices, people have become subjects to public exposure. Platforms mitigate the easy flow of information with a full visibility to social media. Trottier (2011) identifies that as a new level of capital and control which called as "leveling of hierarchy of surveillance". To explain, Facebook services, for instance, give users control over who can see information from their connections and not from the platform itself; you can manage your privacy and security through twelve options, none of which prevent Facebook from collecting your data, (Facebook, 2022).

Yet, users' willingness to share their information or data with these platforms is based on how they perceive their data will be used for. A significant relationship was found between the user's perception of surveillance and their desire to give their information. To explain, people who perceive that their data is collected to enhance communication and for commercial purposes are more likely to share their data, whereas those who perceive it security measures are less willing to share information and content with social media companies. Twitter and Facebook (Meta) clearly states that "when users create content, all information will be shared with third parties", and when it is required by law to prevent harm in the public sphere, with their affiliates, in case of change in ownership, (Twitter, 2022; Facebook, 2022) .

Despite platforms proclaiming their transparency, the findings indicate that users doubts that the platforms would acknowledge misuse of their information. There is a statistically

significant relationship between users' trust and their willingness to share their information with the social media companies. These results are consistent Wang et.al. (2016) who found that trust plays a vital role in the relationship between platforms and individual behavior on social media platforms, they are having a larger effect than even friends and family. Scandals like Snowden and Cambridge Analytica raised trust problems with these Platforms, as users became aware of potential for their data to be monitored and used. Suspicion only increases with the explosion of the COVID-19 pandemic, where public mapping to identify patients' gender and ages and masking compliance emerged, (Lyon, 2021; Thompson, 2020).

The findings support the important of privacy to the users. People who perceive their privacy as an important element while engaging on these platforms are less likely to provide their data. In other words, to not being monitored and controlling the amount of data accessible by these platforms is a priority. According to Pew Research Center (2018), Americans are worrying about their personal data that is collected on social media. It has been found that 91% of Americans have lost control over how their data is collected and feel insecure as a result (Rainie, 2018). Some people took steps to hide or shield their content while others changed their online behavior to minimize detection.

Further, participants who feel less freedom on social media platforms are more self-censored. Another Pew center survey (2018) found that people who have a sense of being surveilled are using social media less and avoid certain terms in their online communication. A PEN America report surveyed around 800 social media users around the world and found that: writers who are living in democratic states have begun to engage in self-censorship at a similar level to those who are living in non-democratic countries. They have a perception that expressing certain views or searching for certain topics might have negative consequences.

The findings delineated that the intention to resist the social media surveillance is relatively low when people are highly concerned about being surveilled. This could be explained by (Trepte et al. (2020) who found that users' choices have been proven to be complex and contextual. In other words, individual self-disclosure in certain contexts and technological affordance must be taken into account. According to Smith, (2018) users living in "data doxa"- where data is entangled with beliefs of data for security and envision of welfare life- cannot be achieved without data collection. Smith is a little pessimistic about people's ability to make informed and conscious decisions against surveillance of digital services.

Limitations and future studies:

This study comes with some limitations. First, the study utilized quantitative method only, which makes the study lacks deeper explanations and analysis of users' behavior and their perception towards the social media platform policies. Second, the results of this study used a non-random convenient sample, which although could be used as an indicator, it cannot be generalized to the rest of the population.

Further studies could take different angels. First, in-deoth interviews could be conducted with experts to understand their perspective on the different social media platform policies. Second, focus groups with users could be set to better analyze their perception on these policies, third, this study could be duplicated on other Arab countries to measure the similarities and differences of users' perception towards social media platform policies

Reference:

Abdel Meguid, L. (2020). Al-Tanzeem Al-Tashree'i wa Al-Qanouni Lel'lam Al-Taqlidi wa Al-Electroni. Media Regulations and Legislations for the Traditional and Electronic Media. Al-Arabi Press.

Afriat, H., Dvir-Gvirsman, S., Tsuriel, K., & Ivan, L. (2021). "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal. The Information Society, 37(2), 115-127. doi: 10.1080/01972243.2020.1870596

AFTE (2020a) Freedom of Expression in the Time of Social Distancing Quarterly Report on the State of Freedom of Expression in Egypt (January–March 2020), Cairo: Association of Freedom of Thought and Expression (AFTE) (accessed 20 June 2022).

Al Ahram Online, (2018). Retrieved 21 June 2022, from https://english.ahram.org.eg/NewsContent/1/64/111038/Egypt/Politics-/Egypt-begins-close-monitoring-of-online-communicat.aspx.

Al Ahram, (2018). Jail term and EGP 20,000 fine for spreading rumours about coronavirus: Egypt's prosecution. Al Ahram. English.

(2020). Retrieved 21 June 2022fromhttps://english.ahram.org.eg/NewsContent/1/64/366161/Egypt/Politics-/Jail-term-and-EGP-,-fine-for-spreading-rumours-abo.aspx.

Al Khatib, H., & Kayyallia, D. (2019). *Opinion | YouTube Is Erasing History (Published 2019)*. Nytimes.com. Retrieved 4 June 2022, from https://www.nytimes.com/2019/10/23/opinion/syria-youtube-content-moderation.html.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. First Monday.

Alexander v. United States (US Supreme Court 1993).

Andrejevic, M. (2004). The work of watching one another: Lateral surveillance, risk, and governance. Surveillance & Society, 2(4).

Astapova, A. (2017). In Search for Truth: Surveillance Rumors and Vernacular Panopticon in Belarus. *Journal Of American Folklore*, 130(517), 276-304. doi: 10.5406/jamerfolk.130.517.0276

Article 19. (2018). Egypt: 2018 Law on the Organization of Press, Media and the Supreme Council of Media. Legal Analysis. H

ttps://www.Article19.org/wp-content/uploads/2019/03/Egypt-Law-analysis-FinalNov-2018.pdf

June 21, 2022, 12:02 P92

Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management,* 50, 171-181.

Badr, H. (2020). Egypt: A Divided and Restricted Media Landscape after the Transformation. In: Arab Media Systems (215-232). Eds: Carola Richter and Claudia Kozman. Arab German Young Academy.

Ball, K. (2009). Exposure: Exploring the subject of surveillance. Information, Communication & Society, 12(5), 639-657.

Ball, K. (2010). Workplace surveillance: an overview. Labor History, 51(1), 87-106. doi: 10.1080/00236561003654776

Balkin, J. M. (2012). The first amendment is an information policy. *Hofstra L. Rev.*, *41*, 1.

Balkin, J. M. (2018). Free speech is a triangle. *Colum. L. Rev.*, *118*, 2011.

Balkin, J. M. (2017). Free speech in the algorithmic society: big data, private governance, and new school speech regulation. *UCDL Rev.*, *51*, 1149.

Balkin, J. M. (2014). Old-school/new-school speech regulation. *Harvard Law Review, 127(8),* 2296-2342.

Bamberger, K. A. (2010). Technologies of compliance: risk and regulation in digital age. *Texas Law Review, 88(4),* 669-740.

Bashir, M., Hayes, C., Lambert, A. D., & Kesan, J. P. (2015). Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology*, *52*(1), 1-10. https://doi.org/10.1002/pra2.2015.145052010043

Bauman, Z., & Lyon, D. (2013). Liquid surveillance (1st ed.). Cambridge, UK: Polity Press.

Bennett, C., Haggerty, K., Lyon, D., & Steeves, . (2014). *Transparent Lives*. Athabasca University Press. https://dspace.library.uvic.ca/bitstream/handle/1828/10506/Bennett_et_al_2014-Transparent_Lives.pdf?sequence=3&isAllowed=yhttps://dspace.library.uvic.ca/bitstream/handle/1828/10506/Bennett_et_al_2014-Transparent_Lives.pdf?sequence=3&isAllowed=y.(*Civil Rights Cases, 109 U.S. 3 (1883)*,,https://supreme.justia.com/cases/federal/us/109/3/

Bennett, W. L. (2008). Changing citizenship in the digital age.

Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Bridy, A. (2016). Copyright's digital deputies: DMCA-plus enforcement by Internet intermediaries. In *Research handbook on electronic commerce law*. Edward Elgar Publishing.

Brighenti, A. M. (2010). Lines, barred lines. Movement, territory and the law. *International Journal of Law in Context*, 6(3), 217-227.

Bronner v. Duggan, 249 F. Supp. 3d 27, 41 (D.D.C. 2017), https://casetext.com/case/bronner-v-duggan-2

Carr, C. T., & Hayes, R. A. (2015). Social media: Defining, developing, and divining. *Atlantic journal of communication,* 23(1), 46-65.

Cobbe, J. (2019). Algorithmic Censorship by Social Platforms: Power and Resistance.

Cocq, C., Gelfgren, S., Samuelsson, L., & Enbom, J. (2020). Online Surveillance in a Swedish Context: Between acceptance and resistance. Nordicom Review, 41(2), 179-193. doi: 10.2478/nor-2020-0022

ÇÖMLEKÇİ, M. F. (2020). Social Media Use Among International Students: Cultural Adaptation and Socialization.

Corera, G. (2013). Edward Snowden revelations: Can we trust the spying state? BBC News. Retrieved 4 June 2022, from .https://www.bbc.com/news/technology-24399213.

Correia, J., & Compeau, D. (2017, January). Information privacy awareness (IPA): a review of the use, definition and measurement of IPA. In Proceedings of the 50th Hawaii International Conference on System Sciences.

Custers, B., van der Hof, S., & Schermer, B. (2014). Privacy expectations of social media users: The role of informed consent in privacy policies. *Policy & Internet*, *6*(3), 268-295. https://onlinelibrary.wiley.com/doi/epdf/10.1002/1944-2866.POI366

Data.europa.eu. (2015). Retrieved 15 June 2022, from https://data.europa.eu/data/datasets/s2075_83_1_431_eng?locale=en

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*, 11, 763-781.

Diamond, L. (2010). Liberation Technology. *Journal Of Democracy*, *21*(3), 69-83. https://doi.org/10.1353/jod.0.0190

DOCUMENTARY: Edward Snowden - Terminal F (2015). 2022. [Label Worx (on behalf of Kaiseki Digital); UMPG Publishing,]. https://www.youtube.com/watch?v=Nd6qN167wKo

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. New Media & Society, 21(8), 1824–1839. https://doi.org/10.1177/1461444819833331

Duffy, B. E., & Chan, N. K. (2019). "You never really know who's looking": Imagined surveillance across social media platforms. New Media & Society, 21(1), 119-138.

Echikson, W., & Knodt, O. (2022). Germany's NetzDG: A Key Test for Combatting Online Hate. Retrieved 14 June 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3300636

Enforcing new rules to reduce hateful conduct and abusive behavior. (2017). Retrieved 14 June 2022, from https://blog.twitter.com/en_us/topics/company/2017/safetypoliciesdec2017

Elkin-Koren, N. (2020). Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence. *Primary Dental Journal*, 32–36. https://doi.org/10.1177/2050168420911027

Ericson, R. V., Haggerty, K. D., & Murphy, C. (2000). Policing the risk society. *Canadian Journal of Sociology*, 25(1), 111.

Eskandar, W., 2022. How Twitter is gagging Arabic users and acting as morality police. [online] openDemocracy. Available at: <https://www.opendemocracy.net/en/north-africa-west-asia/how-twitter-gagging-arabic-users-and-acting-morality-police/> [Accessed 6 September 2022].

EuroMid rights. (2020). *Dangerous liaisons: Social media as a (flawed) tool of resistance in Egypt*. Retrieved from https://euromedrights.org/wp-content/uploads/2020/09/Study_on_social_media_in_Egypt.pdf

Evans, D., & Schmalensee, R. (2015). *The Antitrust Analysis of Multisided Platform Businesses* (1st ed.). The Oxford Handbook of International Antitrust Economics. DOI: 10.1093/oxfordhb/9780199859191.013.001

Evens, T., & Van Damme, K. (2016). Consumers' willingness to share personal data: Implications for newspapers' business models. *International journal on media management*, 18(1), 25-41.

Facebook | Facebook. Perma.cc. (2004). Retrieved 25 December 2021, from https://perma.cc/3ZV5-MECX

Facebook adds an "Ask" button for flirting, nagging and more. (2014). Retrieved 14 June 2022, from http://www.cbsnews.com/news/facebook-adds-ask-button-for-flirting-nagging-and-more/

Facebook Privacy Basics. (2022). Retrieved 15 June 2022, from https://www.facebook.com/about/basics/manage-your-privacy\

"Facebook users in Egypt":| Meta Business Help Centre. Meta Business Help Centre. (2022). Retrieved 21 June 2022, from https://www.facebook.com/business/help/search/?query=Facebook%20users%20in%20Egypt&ssid=fdShO3BgadYLsFZ.

Farahat, M. (2021a) Coronavirus Trials in Egypt: Blurring the Lines Between Fake News and Freedom of Expression, SMEX (accessed 4 August 2021)

Farr, (2018). *Here's everything you need to know about the Cambridge Analytica scandal*. [online] CNBC. Available at: <https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html> [Accessed 21 July 2022].

Fatima, T., & Bilal, A. R. (2019). Achieving SME performance through individual entrepreneurial orientation: An active social networking perspective. *Journal of Entrepreneurship in Emerging Economies*.

Filistrucchi, L., Geradin, D., & van Damme, E. (2012). Identifying Two-Sided Markets. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2008661

Finn, J. (2013). Seeing surveillantly: surveillance as social practice. In Eyes Everywhere (pp. 83-96). Routledge.

Foucault, M., & Kritzman, L. (2013). *Politics, philosophy, culture: Interviews and other writings, 1977-1984*. Routledge.

Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (Eds.). (2013). Internet and surveillance: The challenges of Web 2.0 and social media (Vol. 16). Routledge.

Fuchs, C. (2015). Surveillance and Critical Theory. *Media And Communication*, *3*(2), 6-9. https://doi.org/10.17645/mac.v3i2.207

Fussey, P. (2007). An interrupted transmission? Processes of CCTV implementation and the impact of human agency. *Surveillance & Society*, *4*(3). http://www.surveillance-and-society.org/

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. MIS Quarterly, 27(1), 51e90

Gellman, B., & Poitras, L. (2013). *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*. The Washington post. Retrieved 18 July 2022, from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Gillespie, T. (2018). Custodians of the Internet. In *Custodians of the Internet*. Yale University Press.

Gibbs, S. (2016). US border control could start asking for your social media accounts. Retrieved 15 June 2022, from https://www.theguardian.com/technology/2016/jun/28/us-customs-border-protection-social-media-accounts-facebook-twitter

Gozalishvili, N. (2021). The Contested Triangle of Disinformation, Democratization and Populism in Georgia. democratization, 23, 02

Grimmelmann, J. (2015). The Virtues of Moderation. *Yale Journal of Law and Technology, 17,* 42-109.

Graham, S., & Wood, D. (2017). Digitizing surveillance: categorization, space, inequality. In Surveillance, crime and social control (pp. 537-558). Routledge.

Greenwald, G., & Gallagher, R. (2014). New Zealand launched mass surveillance project while publicly denying it. The Intercept, 15.

Halliday, J. (2012). Twitter's Tony Wang: 'We are the free speech wing of the free speech party'. the Guardian. Retrieved 25 December 2021, from https://www.theguardian.com/media/2012/mar/22/twitter-tony-wang-free-speech

Harcourt, B. E. (2015). Exposed: Desire and disobedience in the digital age. Harvard University Press.

Hargittai, E., & Litt, E. (2013). New strategies for employment? internet skills and online privacy practices during people's job search. *IEEE Security &Amp; Privacy*, *11*(3), 38-45. doi: 10.1109/msp.2013.64

Hassanin, L. (2014) Global Information Society Watch 2014, APC and HivosHassanin, L. (2014) Global Information Society Watch 2014, APC and Hivos

Heldt, A. (2019). Upload-filers: bypassing classical concepts of censorship. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 10(1),* 56-64.

Hintz, A. (2014). Outsourcing Surveillance—Privatising Policy: Communications Regulation by Commercial Intermediaries. *Birkbeck Law Review Volume*, *2(2)*. Retrieved 4 June 2022, from https://orca.cardiff.ac.uk/id/eprint/70838/1/349_Outsourcing-Surveillance-Privatising-Policy_2014-12-06.pdf.

Hooker, M. P. (2019). Censorship, Free Speech & Facebook: Applying the First Amendment to Social Media Platforms via the Public Function Exception. *Wash. JL Tech. & Arts*, *15*, 36.

Humphreys, L. (2011). Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication,* 61(4), 575-595.

Inc., H. (2022). *Digital 2021 Report (October Update)*. Hootsuite. Retrieved 4 June 2022, from https://www.hootsuite.com/resources/digital-trends-q4-update.

Jeffries, A. (2013). Escape from PRISM: how Twitter defies government data-sharing. Retrieved 14 June 2022, from https://www.theverge.com/2013/6/13/4426420/twitter-prism-alex-macgillivray-NSA-government

Jeong, S. (2016). The History of Twitter's Rules. Retrieved 14 June 2022, from https://www.vice.com/en/article/z43xw3/the-history-of-twitters-rules

Jeong et alJiang, L. C., Bazarova, N. N., & Hancock, J. T. (2011). The disclosure–intimacy link in computer-mediated communication: An attributional extension of the hyperpersonal model. 37(1), 58-77.

Jurgenson, N. 2013. Review of Bauman and Lyon's Liquid Surveillance: A Conversation. *Surveillance & Society* 11(1/2): 204-207

Kan, M. (2019). Facebook Taps Next-Gen AI To Help It Detect Hate Speech. Retrieved 14 June 2022, from https://www.pcmag.com/news/facebook-taps-next-gen-ai-to-help-it-detect-hate-speech

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business horizons, 53(1), 59-68.

Katsh, M. E., & Rabinovich-Einy, O. (2017). *Digital justice: technology and the internet of disputes*. *Oxford University Press.*

Klonick, K. (2017). The new governors: The people, rules, and processes governing online speech. *Harv. L. Rev.*, *131*, 1598

Klonick, K. (2018). The New Governors: The People, Rules, and Processes Governing Online Speech. *Harvard Law Review, 131(6),* 1598-1670.

Hanna K., S. (2018). The Cambridge Analytica scandal is wildly confusing. This timeline will help. Retrieved 14 June 2022, from https://qz.com/1240039/the-cambridge-analytica-scandal-is-confusing-this-timeline-will-help/

Khumaryan, D. (2019). Nick Srnicek's Platform Capitalism: Crisis — Response — Boom — Crisis — and Response Again. What Do We Know about the Digital Economy? Book Review: Srnicek N. (2019)

Kapitalizm platform [Platform Capitalism] (Russian transl. by Maria Dobryakova), Moscow: HSE Publishing House (in Russian). *Journal Of Economic Sociology*, *20*(3), 164-179. https://doi.org/10.17323/1726-3247-2019-3-164-179

Langvardt, K. (2018). Regulating online content moderation. *Georgetown Law Journal, 106(5),* 1353-1388.

Lessig, L. (2006). *Code Version 2.0*. 2nd ed. New York: Basic Books A Member of the Perseus Books Group, p.19.

Longhurst, B. (1990). Raymond Williams: The sociological legacy. Sociology, 24(3), 519-527.

Lupton, D. (2014). *Digital sociology*. Routledge.

Lynch, M. (2011). After Egypt: The limits and promise of online challenges to the authoritarian Arab state. *Perspectives on politics*, *9*(2), 301-310.

Lyon, D. (2017). Digital citizenship and surveillance| Surveillance culture: engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, 11, 19.

Lyon, D. (Ed.). (2003). Surveillance as social sorting: Privacy, risk, and digital discrimination. Psychology Press.

Lyon, D. (2001). *Surveillance society*. McGraw-Hill Education (UK).

Lyon, D. (2014a). Surveillance, Snowden and Big Data: Capacities, Consequences, Critique, Big Data & Society 1(1), 1-13

Lyon, D. (Ed.). (2003). Surveillance as social sorting: Privacy, risk, and digital discrimination. Psychology Press.

Lyon, D. (2021). Surveillance, transparency, and trust. Trust and Transparency in an Age of Surveillance, 243.

Mani, Z., & Chouk, I. (2019). Impact of privacy concerns on resistance to smart services: does the 'Big Brother effect' matter?. *Journal Of Marketing Management*, 35(15-16), 1460-1479. doi: 10.1080/0267257x.2019.1667856

Marx, G. T. (2016). Windows into the soul. University of Chicago Press.

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society*, 9(4), 378-393.

McGrath, J. E. (2004). Loving Big Brother: Performance, privacy and surveillance space. Psychology Press.

Meredith, S., 2018. Here's everything you need to know about the Cambridge Analytica scandal. [online] CNBC. Available at: <https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html> [Accessed 21 July 2022].

Mikal, J., Rice, R., Kent, R., & Uchino, B. (2014). Common voice: Analysis of behavior modification and content convergence in a popular online community. *Computers In Human Behavior*, *35*, 506-515. https://doi.org/10.1016/j.chb.2014.02.036

Moss, C. (2014). Twitter Is Changing Its Policies Following Harassment Of Robin Williams' Daughter. Retrieved 14 June 2022, from https://www.businessinsider.com/twitter-policies-change-for-zelda-williams-2014-8

Nelson, M. K., & Garey, A. I. (Eds.). (2009). *Who's Watching?: Daily Practices of Surveillance among Contemporary Families* (p. 298). Nashville, TN: Vanderbilt University Press.

NGOs call on Facebook to stop censoring Palestinian content and get rid of an Israeli Oversight Board member. (2020). Retrieved 4 June 2022, from https://english.wafa.ps/Pages/Details/120346.

Norris, C., & Armstrong, G. (2020). *The maximum surveillance society: The rise of CCTV*. Routledge.

Ofcom (2019) The use of AI in content moderation. Report produced by Cambridge Consultants on behalf of Ofcom. Available at: www.ofcom.org.uk/__data/assets/pdf_file/ 0028/157249/cambridge-consultants-ai-content-moderation.pdf (accessed 12 February 2022)

OHCHR | International Covenant on Civil and Political Rights. Previous.ohchr.org. (2022). Retrieved 30 May 2022, from https://previous.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

Open Technology Fund Information Controls. (2019). *Digital Authoritarianism in Egypt Digital Expression Arrests 2011-2019*. Retrieved from https://public.opentech.fund/documents/EgyptReportV06.pdf

Oreskovic, A. (2012). Facebook to share data with Instagram, loosen email rules. Retrieved 14 June 2022, from https://www.reuters.com/article/us-facebook-privacy/facebook-to-share-data-with-instagram-loosen-email-rules-idUSBRE8AK18E20121121

O'Sullivan, P. B. (2005, May). Mass personal communication: Rethinking the mass interpersonal divide. Paper presented at the annual meeting of the International Communication Association, New York, NY

Paramarta, V., Jihad, M., Dharma, A., Hapsari, I. C., Sandhyaduhita, P. I., & Hidayanto, A. N. (2018, October). Impact of user awareness, trust, and privacy concerns on sharing personal information on social media: Facebook, twitter, and instagram. In *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (pp. 271-276). IEEE. DOI:10.1109/ICACSIS.2018.8618220

Park, Y. (2021). Structural Logic of AI Surveillance and Its Normalisation in the Public Sphere. Javnost - The Public, 28(4), 341-357. doi: 10.1080/13183222.2021.1955323

Parr, B. (2011). Facebook's Big Privacy Changes: An Overview [PICS]. Retrieved 14 June 2022, from https://mashable.com/archive/facebook-privacy-changes-guide#TMdc0NovxZqX

PEN American Center. (2015). GLOBAL CHILLINGThe Impact of Mass Surveillance on International Writers. Retrieved from https://pen.org/sites/default/files/globalchilling_2015.pdf

Paul, K. (2022). US supreme court blocks Texas law targeting social media rules. Retrieved 14 June 2022, from https://www.theguardian.com/media/2022/may/31/texas-social-media-law-supreme-court

Penney, J. (2017). Internet surveillance, regulation, and chilling effects online: a comparative case study. Internet Policy Review, 6(2). doi: 10.14763/2017.2.692

Ping Yu, R. (2021). The Emergence of Surveillance Culture: The Relationships between Facebook Privacy Management, Online Government Surveillance, and Online Political Expression. *Journal Of Broadcasting &Amp; Electronic Media*, 65(1), 66-87. doi: 10.1080/08838151.2021.1897816

Post, T. (2021). *Rights group cites Facebook 'censorship' of Palestinians*. The Jakarta Post. Retrieved 4 June 2022, from https://www.thejakartapost.com/world/2021/10/10/rights-group-cites-facebook-censorship-of-palestinians-.html.

Plantin, J., Lagoze, C., Edwards, P., & Sandvig, C. (2016). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media &Amp; Society*, *20*(1), 293-310. doi: 10.1177/1461444816661553

Putman, R. (2020). Manhattan Community Access Corp. v. Halleck. *Ohio NUL Rev.*, *46*, 195.

Rainie, L. (2018). Americans' complicated feelings about social media in an era of privacy concerns. Retrieved 15 June 2022, from https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Roberts, N. (2015). Freedom as marronage. In Freedom as Marronage. University of Chicago Press.

Rosen, J. (2013). The Delete Squad. The New Republic. Retrieved 28 December 2021, from https://newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules

Rule, J. (1973). *Private lives and public surveillance*. London: Allen Lane.

Egypt targets social media with new law. Reuters. (2018). Retrieved 21 June 2022, from https://www.reuters.com/article/us-egypt-politics-idUSKBN1K722C.

Russo, A., Watkins, J., Kelly, L., & Chan, S. (2008). Participatory communication with social media. *Curator: The Museum Journal*, *51*(1), 21-31.

Sengupta, S.(2012). Twitter's Free Speech Defender (Published 2012). [online] Nytimes.com. Available at: <https://www.nytimes.com/2012/09/03/technology/twitter-chief-lawyer-alexander-macgillivray-defender-free-speech.html> [Accessed 23 December 2021].

Smith, G. J. (2018). Data doxa: The affective consequences of data practices. Big Data & Society, 5(1), 1–15. https://doi.org/10.1177%2F2053951717751551

Solon, O. (2021). *Pro-Palestinian activists target Facebook with 1-star app store reviews*. NBC News. Retrieved 4 June 2022, from https://www.nbcnews.com/tech/social-media/pro-palestinian-activists-target-facebook-1-star-app-store-reviews-n1268258.

Solum, L. (2009). Legal theory lexicon: Rules, standards, and principles. *Legal Theory Blog*,

Staples, W. G. (2000). Everyday surveillance: Vigilance and visibility in postmodern life. Lanham, Md. [u.a.] : Rowman & Littlefield.

Steinkuehler, C. A., & Williams, D. (2006). Where everybody knows your (screen) name: Online games as "third places". *Journal of computer-mediated communication*, *11*(4), 885-909.

Stoddart, E. (2012). A surveillance of care: Evaluating surveillance ethically. In K. Ball, K. Haggerty, & D.

Stutzman, F. D., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of privacy and confidentiality*, 4(2), 2.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly*, 93(2), 296-311.

Sundar, S. (2012). Social psychology of interactivity in human-website interaction. In Oxford Handbook of Internet Psychology Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199561803.013.0007

Sutton, A., & Wilson, D. (2002). Open-Street CCTV in Australia: The Politics of Resistance and Expansion. Surveillance &Amp; Society, 2(2/3). doi: 10.24908/ss.v2i2/3.3380

Suzor, N. P. (2019). Lawless: The secret rules that govern our digital lives. *Cambridge University Press.*

T. Car, C., & A. Hayes, R. (2022). Social Media: Defining, Developing, and Divining. *Atlantic Journal of Communication,* https://doi.org/DOI: 10.1080/15456870.2015.972282

The Communications Decency Act 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material. https://www.law.cornell.edu/uscode/text/47/230

The ICO for the European conference of Data Protection Authorities, Manchester - May 2015. (2015). Data protection rights: What the public want and what the public want from Data Protection Authorities (pp. 3-7). Manchester. Retrieved from https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf

Taylor, C. (2004). On social imaginary. *C. Taylor, Modern Social Imaginaries*, 23-30.

Thompson, D. (2022). What's Behind South Korea's COVID-19 Exceptionalism?. Retrieved 15 June 2022, from https://www.theatlantic.com/ideas/archive/2020/05/whats-south-koreas-secret/611215/

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of af-fordances. Computers in Human Behavior, 104, 106115. https://doi.org/10.1016/j.chb.2019.08.022.

Twitter, (2019). New disclosures to our archive of state-backed information operations. (Retrieved 14 June 2022, from https://blog.twitter.com/en_us/topics/company/2019/new-disclosures-to-our-archive-of-state-backed-information-operations

Twitter, (2021). Expanding our private information policy to include the media. (2021). Retrieved 14 June 2022, from https://blog.twitter.com/en_us/topics/company/2021/private-information-policy-update

Twitter Privacy Policy. (2022). Retrieved 15 June 2022, from https://twitter.com/en/privacy

Twitter, (2021). Updates to our work on COVID-19 vaccine misinformation. (2021). Retrieved 14 June 2022, from https://blog.twitter.com/en_us/topics/company/2021/updates-to-our-work-on-covid-19-vaccine-misinformation

Trottier, D. (2016). Social media as surveillance: Rethinking visibility in a converging world. Routledge.

Trottier, D. (2011). A Research Agenda for Social Media Surveillance. Fast Capitalism, 8(1), 59-68. https://doi.org/10.32855/fcapital.201101.008

Tsukayama, H. (2013). Facebook privacy: Users should check these settings as new changes roll out. Retrieved 14 June 2022, from https://www.washingtonpost.com/business/technology/facebook-privacy-users-should-check-these-settings-as-new-changes-roll-out/2013/10/11/4a3ef4e2-3274-11e3-89ae-16e186e117d8_story.html

Tuunainen, V. K., Pitkänen, O., & Hovi, M. (2009). Users' awareness of privacy on online social networking sites-case facebook. *Bled 2009 proceedings*, 42. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1000&context=bled2009

Alsenoy, B., Verdoodt, V., Heyman, R., Ausloos, J., Wauters, E., & Acar, G. (2015). *From social media service to advertising network - A critical analysis of Facebook's Revised Policies and Terms. Retrieved from https://www.researchgate.net/profile/JefAusloos/publication/291147719_From_social_media_service_to_advertising_network__A_critical_analysis_of_Facebook%27s_Revised_Policies_and_Terms/links/569e4a80*

08aed181045fdfac/From-social-media-service-to-advertising-network-A-critical-analysis-of-Facebooks-Revised-Policies-and-Terms.pdf?origin=publication_detail

Vladeck, D (2018) Facebook, Cambridge Analytica, and the regulator's dilemma: Clueless or Venal? *Harvard Law Review Blog*. Available at: https://blog.harvardlawreview.org/facebook-cambridge-analytica-and-the-regulators-dilemma-clueless-or-venal/ (accessed 25 October 2019).
Google Scholar

Visual Capitalist. (2021). *Ranked: The World's Most Popular Social Networks, and Who Owns Them*. [online] Available at: <https://www.visualcapitalist.com/ranked-social-networks-worldwide-by-users/> [Accessed 18 December 2021]. (Ranked: The World's Most Popular Social Networks, and Who Owns Them, 2021) In-text citation: (Ang, 2021), https://www.visualcapitalist.com/ranked-social-networks-worldwide-by-users/

Wahl-Jorgensen, K., Bennett, L., & Cable, J. (2016). Surveillance Normalization and Critique. *Digital Journalism*, 5(3), 386-403. doi: 10.1080/21670811.2016.1250607

Wang, V., & Tucker, J. (2021). 'I am not a number': Conceptualising identity in digital surveillance. Technology In Society, 67, 101772. doi: 10.1016/j.techsoc.2021.101772

Wang, Y., Min, Q., & Han, S. (2016). Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence. Computers in Human Behavior, 56, 34-44.

Weiss, M. A,(2021). Regulating Freedom of Speech on social media: Comparing the EU and US

Womah Mukong v. Cameroon, Communication No. 458/1991, U.N. Doc. CCPR/C/51/D/458/1991 (1994). (1991). Cameroon.

Wu, F. T. (2011). Collateral Censorship and the Limits of Intermediary Immunity. Notre Dame L. Rev., 87, 293. https://scholarship.law.nd.edu/ndlr/vol87/iss1/6/

Wu, supra note 3, at 295–96, CIRCUIT, F. A. C. F. F. DISCLOSURE LAW. -Washington Post v. McManus, 944 3 d 5o6 (4 the Womah Mukong v. Cameroon, , (1994). Cameroon.

Wylie, C. (2018). Whistleblower Christopher Wylie says he's now been blocked by Facebook Retrieved from: [https://www.cnbc.com/2018/03/18/whistleblower-christopher-wylie-says-hes-now-been-blocked-by-facebook.html].

Young v. Facebook, Inc., Case Number 5:10-cv-03579-JF/PVT (N.D. Cal. Oct. 25, 2010) [Facebook, Inc., No. 5:10–cv–03579–JF/PVT, 2010 WL. 4269304, at *2–3 (N.D. Cal. Oct. 25, 2010) (dismissing plaintiff's Section 1983. First Amendment claim)]

Zeran, 129 F.3d at 331., 97-1523 AMERICA ONLINE, INCORPORATED, Defendant-Appellee 331 (1997).

Zhang, D. Y., Li, Q., Tong, H., Badilla, J., Zhang, Y., & Wang, D. (2018, August). Crowdsourcing-based copyright infringement detection in live video streams. In *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 367-374). IEEE.

Zolait, A. H. S., Al-Anizi, R. R., Ababneh, S., BuAsalli, F., & Butaiba, N. (2014). User awareness of social media security: the public sector framework. *International Journal of Business Information Systems*, 17(3), 261-282.

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal Of Information Technology*, *30*(1), 75-89. doi: 10.1057/jit.2015.5

Zureik, E., Stalker, L., Smith, E., Lyon, D., & Chan, Y. (2010). Surveillance, privacy, and the globalization of personal information (1st ed.). McGill-Queen's University Press

Appendix 1:

Social media policies change:

.

	Facebook
Definition as it is in the platform	Facebook helps you connect with friends, family, and communities of people who share your interests. Connecting with your friends and family as well as discovering new ones is easy with features like Groups, Watch, and Marketplace
2008	**Users become able to limit the audience:** ➢ Some personal information is private ➢ A person's full name, gender, and city should be public in the platform list, (Keys, 2018)
2009	
2010	**Data for third party websites**: ➢ Facebook began offering up user data to third party websites and services. ➢ The company wrote out a new privacy policy that clocked in at 5,830 words Facebook said users could opt out of sharing most of their personal data with third parties, ➢ Critic: The option to restrict data sharing was disabled by default. (New York Times, 2010)
2011	**New privacy policies**: ➢ No option for preventing friends from tagging on location. ➢ Critics: confusing and required users to watch tutorials to explain the new policies, Electronic Frontier Foundation, (Parr, **, 2011)**
2012	**Privacy policy to grant the company a blanket right to materials uploaded by its users.** ➢ Allowed the platforms to use the material to deliver targeted ads to users. ➢ Eliminated a feature that allowed users to restrict who could contact them on the site. ➢ Critics: Unify user-profiles between Facebook and Instagram, a move that "could open the door for Facebook to build unified profiles of its users that include people's personal data from its social network." Reuters

2013 The Snowden leaks	**The scandal broke in early 2013 and revealed that the US National security Agency (NSA) tapped directly into the servers of nine internet firms including Facebook, Google Microsoft, and Yahoo <u>except Twitter</u> to track online communication in a surveillance program called US - UK Prism Program. (BBC, 2013)**
2013	**Facebook:** ➢ Allowed users to mass restrict prior posts. At the same time, ➢ Removed an option that allows users to hide their profiles from searches. ➢ <u>Critics</u>: Facebook's intention was to force users to "control their privacy on an item-by-item basis." ➢ Data the company could then use internally and funnel to third parties, The Washington Post, 2013
2014	**Change Private policy:** ➢ Company acknowledged that it seeks to make money of appropriating material uploaded by its users. ➢ Rolled out a feature that encouraged users to "ask" their connections to input more private information on their profiles, CBS news. 2014.
2015	1. **Consent:** ➢ It is considered the only viable justification for Facebook's processing activities. It gives limited information to users with no meaningful choice regarding certain processing operations. Critics: not specified, ambiguous. 2. **Privacy settings**: (<u>Critics</u>) ➢ Consent cannot be inferred from the data inaction regarding behavioral marketing. ➢ Facebook's opt system for advertising does not meet the requirements for legally valid consent. ➢ Collection of location data and "sponsored stories opt-outs are not provided for users. 3. **Unfair contract terms**: ➢ Facebook's SRR contains several provisions which do not comply with the Unfair Contract Terms Directive. 4. **How Facebook" combines and shares data about its users:**

	➢ Facebook has a wide variety of sources (Instagram, What's App and data brokers) where it can combine data from. It can gain a deeper detailed profile of its users. ➢ Critics: It provided such profiles for third party advertising purposes; a practice does not meet the reequipment for legal valid consent. 5. **Further use of generated content:** ➢ Facebook allows the company to generate content for commercial purposes (e.g., sponsored stories, social ads) ➢ Critics: a practice that is not transparent for users in its consent, with no control mechanism for the user to know when their data collected or what are the purposes for this data collection. 6. **Location:** ➢ Facebook collects location data from a variety of sources. The only way to stop Facebook mobile app from accessing location data on one's smartphone is to do so at the level of the mobile operating system 7. **Tracking:** ➢ Facebook is monitoring its users with a high-level information tracking practice, no free and prior informed consent before storing or accessing information on an individual device. Rather, Facebook tracks nonusers which are against e. privacy directive. 8. **Data Subject rights: (critics)** ➢ Facebook terms do not properly acknowledge the data subject rights of its users. With no complete overview of all data collected, nor the uses of data (Van Alsenoy et al., 2015)
2016	In December 2016, Facebook, Microsoft, Twitter, and YouTube partnered to "curb the spread of terrorist content online" to create a shared industry database of "hashes," described as "unique digital "fingerprints... for violent terrorist imagery or terrorist recruitment videos or images by which the platform removes this content easily.
2018	Facebook, Google, Twitter, and Mozilla signed an EU Code of Practice on Disinformation in October 2018 and each presented a roadmap to implement the Code. Microsoft signed it in May 2019, and TikTok in June 2020.
2018After Cambridge	**Face recognition:** ➢ Recognizing people's face which scans every photo uploaded to search for faces and compare them in their database to identify users. Facebook claims: the identification process happens only through explicit consent,

Analytic a scandal	➢ Critics: users for whom face recognition was activated received a notice but were not asked for consent. Photo tag is the automatically opt-in feature assuming that they want face recognition identification. **Privacy setting is default:** (Critics) ➢ users' friend list is publicity visible, even after user's limit who can see lists. The probability search by phone number between Facebook-owned messaging systems; Facebook Massager, WhatsApp, and Instagram **Facebook Targeting practices:** ➢ Facebook's default ad settings involve the profiling of new users based on their relationship status, job title, employer, and education (see new account settings below). Critics: Those defaults are clearly incompatible with the GDPR's "privacy by default" requirement. However, Facebook added Ad Preferences tool, users cannot decide whether they want to see ads that are targeted at them based on their interests and personal data. **Special categories of data:** ➢ Facebook defines a special category of data that includes racial or ethnic, pollical opinion, religious beliefs, health, sexual orientation, and biometric data. Facebook says that "without the user's explicit consent to use such special categories of data, they will be deleted from respective profiles and Facebook's servers. **Right to access and modify users' profile on the platform**: ➢ According to Facebook, DYI provides the user with all the data each user provided on the platform. But as explained above, this does not include information inferred by the platform based on user behavior, posts, comments, likes and so on, nor information provided by friends or other users, such as tags in photos or posts
2019	Twitter, Facebook, Microsoft and YouTube, Instagram, Google+, Dailymotion, Snap and Jeuxvideo.com joined the Code of Conduct scheme in 2018 and 2019; The code of conduct cited the European Union Council Framework Decision 2008/913/JHA of November 28, 2008, on combating certain forms and expressions of racism and xenophobia by means of criminal law. By signing this code, the platforms agreed to remove illegal hate speech in less than 24 hours, with no judicial oversight. Such decisions must be made every day and is carried out by algorithms, by employees, and by outside contractors.
	The June 2019 progress report on Facebook's Civil Rights Audit Report ➢ Announced that Facebook would create an Oversight Board (the Oversight Board) to allow its users to appeal content decisions to Board. The progress report explained that Facebook's goal was "to

	establish a body with independent judgment whose decisions are transparent and binding to review some of the most challenging content decisions that Facebook makes.”
2020	**Independent Oversight Board:** ➢ July 2020 the creation of composed of forty members, which would review content removal decisions and decide if the content should stay published or not.
After COVID-19 Pandemic	**Fake news:** ➢ Facebook’s Community Standard also forbids posting “false news” on the platform. It states that there is "a fine line between false news and satire or opinion,” and this is why the platform does not remove false news, but instead, “significantly reduce[s] its distribution by showing it lower in the News Feed ➢ On October 12, 2020, Facebook announced that it had updated its hate speech policy to prohibit any content denying or distorting the Holocaust

	YouTube
Definition as it is in the platform	“Our mission is to give everyone a voice and show them the world. We believe that everyone deserves to have a voice, and that the world is a better place when we listen, share and build community through our stories”
2007	**YouTube Monetization policies:** ➢ Launch of YPP program by sharing the revenue generated with content creators ➢ Video identification launched to help copyright owners
2010	**Enforcing policies:** ➢ Launch of a new appeal process to help creators in contest community guidelines
2012	**Trust flagger added:** ➢ Providing specialized tools to help experts partner identify harmful content
2013 The Snowden leaks	**The scandal broke in early 2013 and revealed that the US National security Agency (NSA) tapped directly into the servers of nine internet firms including Facebook, Google Microsoft, and Yahoo <u>except Twitter</u> to track online communication in a surveillance program called US -UK Prism Program. (BBC, 2013)**
2013	**Standing up to hate and harassment:** ➢ New tools to enable creators to moderate their own comments
2015	**Foster Child safety:** ➢ Launch of YouTube kids- app designed for kids to give families a safer and simpler viewing experiences. Parents are given the ability to block channels.

2016	**Twitter highlighted that it is not cooperating with Prism**. ➢ Macgillivray… 'doesn't give a shit' when the government comes knocking with demands and intimidation, (Eldh, 2013) **Report abuse button**: ➢ Targeted Abuse policy added to
2017	**Free speech policies overlapping: (Moss, 2014):** The number of Accounts is suspended violating platform rules upon Robin Williams' Daughter's harassment incident
2018	**Twitter should be safe policies:** ➢ an expansion of the ban on pornographic profile, header, and background images. The ban now also included "excessively violent media." ➢ Reformulated indirect threats to clarify what they are and ➢ Some measure taken to help users to report against hate speech, terrorism content, harassment revenge porn, Twitter archive, 2015
2018After Cambridge Analytica scandal	
2019	In December 2016, Facebook, Microsoft, Twitter, and YouTube partnered to "curb the spread of terrorist content online" to create a shared industry database of "hashes," described as "unique digital "fingerprints... for violent terrorist imagery or terrorist recruitment videos or images by which the platform removes this content easily.
	Fighting Misinformation: ➢ Launch of top news shelf in YouTube search results and Breaking news shelf. ➢ Launch of Super chat, giving eligible creators a new way to make money ➢ YPP introduced to verify channels eligibility to monetize ➢ Investing in machine learning systems expands to catch extreme content on a greater scale ➢ Formed GIFCT Global Internet Forum to counter Terrorism ➢ Expanded trusted flagger program to include 35 expert NGOs ➢ Age restrictions were added to content to depict family entertainment characters and child safety policy strengthen to prohibit certain type of content. ➢ Content stated to be raised in search results and watch next

	➢ Machine learning systems expanded to others content areas such as child safety.
2020	
After COVID -19 Pandemic	Hate and harassment polices expanded to prohibit harmful conspiracy theories.
2021	Medical misinformation polices on YouTube are expanded with WHO guideline

	Twitter
Definition as it is in the platform	Twitter is a real-time global information network that lets users create and share ideas and information instantly to serve the public conversation. Twitter is what is happening in the world and what people are talking about right now. When it happens, it happens on Twitter.
2007	
2008	**Trust and safety**: ➢ Twitter declared its transparency policies under the Bill of rights, EU Conversion on Human rights, and UN principles on Business and Human Rights.
2009	**Account verified:** ➢ Twitter dispenses a blue checkmark to celebrities, politicians, corporations, and journalists to identify certain accounts as "real." ➢ Banning trademark infringement on its platform (Jeong, 2016)
2010	**Spamming:** ➢ Of the 447 words added to the Rules, 353 dealt with "spam and abuse"—including selling usernames, selling followers, "following and unfollowing people in a brief time, particularly by automated means," or sending "large numbers of duplicate
2011	**Free speech wing:** ➢ Twitter refused to give data of users' accounts to some governments such as the US, NSA, and England government account revealing **Halliday, 2012**
2012	
2013	

The Snowden leaks	
2013	**Twitter highlighted that it is not cooperating with Prism**. ➢ Macgillivray… 'doesn't give a shit' when the government comes knocking with demands and intimidation, (Eldh, 2013) **Report abuse button**: ➢ Targeted Abuse policy added to
2014	**Free speech policies overlapping: (Moss, 2014):** ➢ The number of Accounts is suspended violating platform rules upon Robin Williams' Daughter's harassment incident
2015	**Twitter should be safe policies:** ➢ an expansion of the ban on pornographic profile, header, and background images. The ban now also included "excessively violent media." ➢ Reformulated indirect threats to clarify what they are and ➢ Some measure taken to help users to report against hate speech, terrorism content, harassment revenge porn, Twitter archive, 2015.
2017	**New Rules on Violence and Physical Harm:** ➢ Specific threats of violence or wishing for serious physical harm, death, or disease to an individual or group of people is in violation of our policies ➢ Any account that uses hateful content will be permanently suspended and be considered sensitive media, (Twitter, 2017)
2018	
2019	
	New disclosures to archive of state-backed information operations: ➢ disclose datasets of information operations the company can reliably link to state actors, data about 5,929 accounts removed for violating our platform manipulation policies for states actors (Most of located in Saudi Arabic (Twitter, 2019) ➢
2020	**Twitter announced in April 2020** ➢ that it would increase its use of machine learning and automation "to take a wide range of actions on

	potentially abusive and manipulative content
After COVID -19 Pandemic	**Fight against Misinformation**: ➢ shared updates on work to protect the public conversation surrounding COVID-19 ➢ applying labels to Tweets that may contain misleading information about COVID-19 vaccines, Twitter, (2021) ➢
2021	**Private media**: ➢ Build tools with privacy and security at the core and expand its scope to include "private media." ➢ People's private information, such as phone numbers, addresses, and IDs, is already not allowed on Twitter. This includes threatening to expose private information or incentivizing others to do so (Twitter, 2021)

Appendix 2

English version of the questionnaire

Potential resistance under the control of social media algorithms, surveillance culture approach in the Egyptian context

1. **Nationality:**
    - Egyptian
    - Other nationalities – Move to end the survey

2. **I have read all information above, and I would like to participate in this study. I know that all information will be anonymous and confidential.**
    - Yes
    - No – Move to the end of the survey

Section 3: People aware of social media surveillance

3. **From 1 to 5, please define to what extant do you engage with social media platforms in your daily life?**

1. 2 3 4 5

4. How many hours do you use social media platforms in a day?
    - 0-1hour
    - 2-4hours
    - 5-7 hours
    - More than 7 hours
5. Do you think that social media platform polices agreement is condition to be active on the platform?
    - Yes
    - No
6. When you read a privacy policy or code of standards, what do you typically do?
    - Read it all the way through in detail
    - Read it part of the way through
    - Glance over it without reading it closely
    - Agree without reading it
7. From 1 -5 define, how much do you feel you understand the laws and regulations that are currently in place to protect your data privacy on social media?

1 2 3 4 5

8. From 1 -5, As far as you know, how much of what you do on social media is being tracked by tech companies?

1 2 3 4 5

9. As far as you know, how much, if any, of what you do on social media accounts are being tracked by social media platforms?

- Zero %
- Less than 10%
- From 10 to 30%
- From 31 to 50%
- From 51 to 70 %
- From 71 to 90%
- From 91 to 100%

10. Do you think that each social media company is creating a data profile for you?

- Yes
- No

Section four: How do individuals perceive social media surveillance?

11. Why do you think Social media platforms aim to collect data?

- For profiling customers and potentially targeting the sale of goods and services to them based on their traits and habits.
  - Yes No May be
- To provide you with the content do you need easily without search
  - Yes No May be
- For the government to collect data about all citizens to assess who might be potential threats.
  - Yes No May be
- To monitor users' posts for signs of depression so they can identify people who are at risk of self-harm and connect them to counseling services.
  - Yes No May be
- Make smart speakers sharing audio recordings of customers with law enforcement to help with criminal investigations.
  - Yes No May be
- To anticipate your behavior in the future.
  - Yes No May be
- Mass manipulation as one of the main aims of surveillance.
  - Yes No May be
- To help government agencies to maintain security

- Yes No May be

- To Help government agencies keep tracking threats to their country
  - Yes No May be
- To maintain country culture
  - Yes No May be

- To have impact on the public opinion
  - Yes No May be

12. To what extent do you have any concerns about the uses of the data collected?

1 2 3 4 5

13. How much do you feel you personally benefit from the data that companies collect about you?

1 2 3 4 5

14. On balance, which would you say most accurately describes how you feel?
    - The benefits I get from companies collecting data about me outweigh the potential risks
    - The potential risks of companies collecting data about me outweigh the benefits
    - No answer

15. How confident are you, if at all, that companies will do the following things?

i. Follow what their privacy policies say they will do with your personal information?

a. 1 2 3 4 5

ii. Promptly notify you if your personal data has been misused or compromised

b. 1 2 3 4 5

iii. Publicly admit mistakes and take responsibility when they misuse or compromise their users' personal data

c. 1 2 3 4 5

Iv. Use your personal information in ways you will feel comfortable with

1 2 3 4 5

V. Be held accountable by the government if they misuse or compromise your data

1 2 3 4 5

16. How comfortable are you, if at all, with companies using your personal data in the following ways?

i. To increase engagement and advertising

1 2 3 4 5

ii.To help improve their fraud prevention systems

1 2 3 4 5

iii.To adjust social media users' behavior

1 2 3 4 5

iv.Government security measures

1 2 3 4 5

v.Avoid harassment

1 2 3 4 5

vi.Social mobilization

1 2 3 4 5

vii.To help you while researching for something

1 2 3 4 5

17. In thinking about all your daily interactions online, please tell us how important each of the following are to you? From 1 to 5 define to what extent these sentences are important to you? 1 is the lowest and 5 is the highest

- Being in control over what kind of information could be shared with social media platforms

  1 2 3 4 5

- Being able to share confidential information on your personal social media accounts

  1 2 3 4 5

- Not feeling someone or machine watch or listen to you without your permission

  1 2 3 4 5

- Sharing your information anonymously

  1 2 3 4 5

- Not receiving ads following your research engine

  1 2 3 4 5

- Not being under the influence of surveillance of the social media algorithm

  1 2 3 4 5

- Not being monitored at your social media accounts

  1 2 3 4 5

18. Do social media platform practice a kind of censorship over your content?

- Yes
- No

19. How did this platform detect its policy over your violation?

- Notified of removing a content due to posting violating content
- Account strike on severity of the content
- Restricted from creating content, such as posting, commenting, using Live or creating a Page.
- Informed that the content might be sensitive or misleading
- Notified that your page or group will be disabled

20. To what extent have you been satisfied with the measures the platform took with you?

1 is less satisfied and 5 most satisfied

1 2 3 4 5

21. In thinking about all your daily interactions online, please tell us how important each of the following to you? From 1 to 5 define to what extent these sentences are important to you? 1 is the lowest and 5 is the highest

- Being able to share content without platform intervening in the your words or point of view

1 2 3 4 5

- Not having someone or machine watch or listen to you without your permission

1 2 3 4 5

- Controlling what information collected from you

1 2 3 4 5

- Not being disrubed by warnings, flagging or spam from the social media platform

1 2 3 4 5

- Not being reviewed at your social media accounts

1 2 3 4 5

Section six: Resistance

22. Have you ever tried to overcome these restrictions/ policies or regulation of social media platforms?

- Yes
- No

23. What are the actions you might do to avoid social media control?

- Switched to different communications channels depending on the information being communicated
- Stop using this app

- Close the app for some time
- Decrease the app rate on the store
- Review and adjust the content in a way that does not be notified by the algorithms
- Use slang language or franco Arabic
- New spellings and repurposed terms and phrases constantly evolve, with new forms of language
- The use of substitute language—replacing officially sanctioned ideological terms with homophonous subversive phrases—to escape internet censorship
- Use of memes, parody, sarcasm, and satire on social platforms often subverting the original meaning of words or phrases through repetition.
- Control the content to be followed the social media regulations

Section eight: general Information

24. Gender:
    - Female
    - Male
25. Age:
    - Less 12 years
    - 13- 18
    - 19-25
    - 26-35
    - 36-45
    - 46-55
    - Above 56 years
26. Education:
    - Primary school
    - Preparatory School
    - Secondary school or Equivalent
    - Bachelor
    - Masters
    - PHD

Arabic Version of the Questionnaire

هل الأفراد العاديون على علم بمراقبة وسائل الإعلام الاجتماعية ؟(الرصد ، خصوصية البيانات والخوارزميات)

1. إلى أي مدى تستخدم منصات التواصل الاجتماعي مثل (فيسبوك ، إنستغرام ، تويتر ، يوتيوب ، تيليجرام ، واتساب ؟
    - دائما
    - غالبا
    - أحيانا
    - نادرا

- أبدا

2. كم مرة يطلب منكم الموافقة على أحكام وشروط سياسة خصوصية الشركة ومدونة المعايير ؟

- دائما
- غالبا
- احيانا
- نادرا
- ابدا

3. عندما يطلب منك الموافقة على سياسة خصوصية الشركة ، كم مرة تقرأها قبل الموافقة عليها ؟
- دائما
- غالبا
- أحيانا
- نادرا
- أبدا

4. عندما تقرأ سياسة الخصوصية أو معايير منصة التواصل الاجتماعي ، ماذا تفعل عادة ؟
- أقرأها بالتفاصيل
- أقرأها جزء منها
- ألقي نظرة سريعة عليها دون قراءة عن كثب
- أوافق دون قراءته

5. إلى أي مدى تشعر أنك تفهم القوانين وسياسات الموجودة حالياً لحماية خصوصية بياناتك على منصات التواصل الاجتماعي؟

- جزء كبير منها
- الكثير منها
- البعض منها
- القليل
- لا شيء منها على الإطلاق

6. على حد علمكم ، كم مما تفعلونه في وسائل التواصل الاجتماعي يتم تعقبه من قبل منصات التواصل الاجتماعي ؟
- كلها
- معظمها
- بعضها
- القليل منها
- لا شيء منها

7. على حد علمكم، كم، إن كان هناك، من أنشطتكم على مواقع التواصل الاجتماعي يتم تتبعهم من قبل الشركات المالكة هذه المنصات؟
- صفر٪
- أقل من 10٪
- من 10 إلى 30٪
- من 31 إلى 50٪
- من 51 إلى 70٪
- من 71 إلى 90٪

- من 91 إلى 100٪

8. هل تعتقد أن كل منصة التواصل الاجتماعي تقوم بإنشاء ملف بيانات خاص بك ؟
   - نعم
   - لا

9. ما هو هدف منصات التواصل الاجتماعي لجمع البيانات ؟
   - زيادة الربح
   - لأسباب أمنية؛ إذا كان من أجل مساعدة حكومات والمسئولين
   - تقديم المساعدة للمستخدمين في حالات الشراء، وتقديم محتوي هم في حاجة إليه

10. من فضلك اختر كل ما تعتقد أنه هدف وراء جمع المعلومات على منصات التواصل الاجتماعي؟
    - لغرض تحديد هوية الزبائن واحتمال استهداف بيع السلع والخدمات لهم على أساس صفاتهم وعاداتهم.
    - لتزويدك بالمحتوى الذي تحتاج بسهولة بدون بحث
    - لكي تقوم الحكومة بجمع البيانات عن جميع المواطنين لتقييم من قد يكون تهديدات محتملة
    - مراقبة سلوكيات المستخدمين لمساعدتهم في حالات المرض النفسي وتقديمه
    - توقع سلوك المستخدمين في المستقبل.
    - التلاعب الجماعي كأحد الأهداف الرئيسية للمراقبة.
    - لتعديل سلوكيات المستخدمين لخلق بيئة إيجابية على المنصة الاجتماعية خالية من الاعتداءات اللفظية أو السلوكيات غير القانونية
    - مساعدة المؤسسات الحكومية على متابعة التهديدات التي يتعرض لها بلدها
    - الحفاظ على الثقافة العامة للمجتمع
    - التأثير على الرأي العام
    - خلق مساحة للتعبير عن الرأي بحرية أمام الجميع دون تفرقة

11. هل لديك أي مخاوف بشأن استخدامات البيانات المجمعة ؟
    - قلق للغاية
    - قلق إلى حد ما
    - قلق بعض الشيء
    - قلق بنسبة معتدلة
    - قلق قليلا
    - غير قلق على الإطلاق

12. إلى أي مدى تشعر أنك شخصيا تستفيد من البيانات التي تجمعها الشركات عنك ؟
    - قدر كبير منها
    - معظمها
    - نسبة معتدلة منها
    - القليل منها
    - لا شيء منها على الاطلاق

13. بالتوازن ، أي من هذه العبارات تصف ما تشعر به فيما يخص مدى الفائدة الشخصية التي تعود عليك من جمع المعلومات؟

- الفوائد التي أحصل عليها من الشركات التي تجمع البيانات عني تفوق المخاطر المحتملة
- المخاطر المحتملة للشركات التي تجمع البيانات عني تفوق الفوائد
- لا إجابة

14. هل من الممكن أن تمر بحياتك اليومية دون جمع عنك من قبل مواقع التواصل الاجتماعي؟
- ممكن الي حد كبير
- ممكن إلى حد ما
- ممكن
- ممكن قليلا
- غير ممكن على الإطلاق

15. إلى أي مدى تثق - إذا كان على الإطلاق - أن الشركات سوف تفعل الأشياء التالية ؟

	غير واثق على الإطلاق	غير واثق قليلاً	واثق	واثق إلى حد ما	واثق للغاية
تتبع ما تقول سياساتهم الخاصة أنهم سيفعلون بمعلوماتك الشخصية					
أبلغك فوراً إذا كانت بياناتك الشخصية قد أسيئت استخدامها أو تعرضت للخطر					
تعترف علنا بالأخطاء وتتحمل المسؤولية عندما تسيء استخدام البيانات الشخصية لمستخدميها أو تخل بها					
نستخدم معلوماتك الشخصية بطرق تجعلك تشارك بياناتك بسهولة					
أن تخضع للمساءلة من قبل الحكومة إذا كانوا يسيئون استخدام أو يعرضون بياناتك للخطر					

16. إلى أي مدى أنت مرتاح مع الشركات التي تستخدم بياناتك الشخصية بالطرق التالية ؟

- - -

	ليست مريحة على الإطلاق	مريحة قليلا	مريحة بعض الشيء	مريحة بشكل معتدل	مريحة للغاية
زيادة المشاركة والإعلان					

المساعدة على تحسين خدماتها					
لتعديل لتعديل سلوك مستخدمي وسائل الإعلام الاجتماعية					
التدابير الأمنية الحكومية					
تعديل سلوكيات المستخدمين على منصاتها					
لمساعدتك أثناء البحث عن شيء ما					

17. ، عند التفكير في جميع تفاعلاتك اليومية عبر الإنترنت؛ يرجى إخبارنا بمدى أهمية كل مما يلي بالنسبة لك.

	مهم جدًا	إلى حد ما مهم	مهم بقدر معتدل	إلى حد ما ليس مهم	ليس مهمًا على الإطلاق
السيطرة على نوع المعلومات التي يمكن مشاركتها مع منصات التواصل الاجتماعي					
القدرة على تبادل المعلومات السرية عن حساباتك الشخصية في وسائط الإعلام الاجتماعية					
لا تشعر أنك مراقب بشخص ما أو ماكينة تشاهد أو تستمع إليك بدون إذنك					
مشاركة معلوماتك مجهولة الهوية					
عدم تلقي إعلانات تتبع محرك بحثك					
ليس تحت تأثير مراقبة خوارزمية وسائل الإعلام الاجتماعية					

عدم مراقبتك في حسابات وسائل الإعلام الاجتماعية الخاصة					

18. الحرية على منصات التواصل الاجتماعي يمكن التعبير عنها بشكل مختلف بين الناس، في كل تفاعلاتك اليومية على الإنترنت ؛ يرجى إخبارنا بمدى أهمية كل من الجمل التالية بالنسبة لك.

	مهم جدًا	إلى حد ما مهم	مهم بقدر معتدل	إلى حد ما ليس مهم	ليس مهمًا على الإطلاق
أن تكون مسيطر على أي منصة تحصل على معلومات عنك					
أن تشارك المحتوى على المنصة دون أن تتدخل في كلماتك أو وجهة نظرك					
عدم وجود شخص ما أو آلة مشاهدة أو الاستماع إليك دون إذنك					
عدم التعرض التحذيرات والتنبيهات أو الرسائل من منصة التواصل الاجتماعي					
لا يتم مراجعتك في حسابات وسائل الإعلام الاجتماعية الخاصة بك					

19. هل سبق وأن تم إخطار انتهاك سياسات محتوى وسائل الإعلام الاجتماعية من قبل ؟
- نعم
- لا

20. كيف أعلمتك هذه المنصة سياستها بخصوص انتهاك ؟
- إخطار بإزالة محتوى بسبب نشر محتوى مخالف
- حظر الحساب لمدة
- ممنوع من إنشاء المحتوى، مثل النشر أو التعليق أو استخدام بث مباشر او إنشاء صفحة
- تم إبلاغه بأن المحتوى قد يكون حساسًا أو مضللًا
- أخطر أن صفحتك أو مجموعتك سيتم تعطيلها

21. إلى أي مدى كنت راضياً عن التدابير التي اتخذتها المنصة معك ؟
- غير راضٍ تمامًا
- غير راضٍ إلى حد ما
- غير راضٍ أو غير راضٍ
- راضٍ إلى حد ما
- راضٍ تمامًا

22. هل حاولت من قبل التغلب على هذه القيود/السياسات أو تنظيم على منصات التواصل الاجتماعي ؟

- نعم
- لا

23. ما هي الإجراءات التي قد تفعلها أو فعلتها لتجنب السيطرة على وسائل الإعلام الاجتماعية ؟ يمكنك اختيار العديد؟

- تحول إلى منصة تواصل اجتماعي مختلفة
- توقف عن استخدام هذا التطبيق
- أغلق التطبيق لبعض الوقت
- خفض معدل تقييم التطبيق على المتجر " Google play, app store "
- استعراض وتعديل المحتوى بطريقة لا يتم الإخطار بها بواسطة الخوارزميات
- استخدم اللغة العامية أو لغة لا يمكن لخوارزميات المنصة ملاحظتها
- استخدام اللغة البديلة ـ الاستعاضة عن العبارات الإيديولوجية المعتمدة رسميا بعبارات مختلفة ـ للهروب من الرقابة على الإنترنت
- استخدام الصور الجرافيك بدل الكلمات ، أو السخرية على المنصة الاجتماعية
- مراقبة المحتوى وفقا لسياسات المنصة
- تجنب مناقشة قضايا معينة على المنصة الاجتماعية

24. النوع ؟

- ذكر
- أنثى

25. السن؟

- أقل من 18 عامًا
- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- فوق 64 سنة

26. المستوى التعليمي؟

- أقل من التعليم الثانوي
- شهادة الثانوية العامة أو ما يعادلها
- درجة البكالوريوس
- الماجستير
- دكتوراة

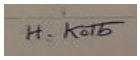
Institutional Review Board Approval:

THE AMERICAN UNIVERSITY IN CAIRO
INSTITUTIONAL REVIEW BOARD

Case# 2021-2022-137

“
”

Please note that IRB approval does not automatically ensure approval by CAPMAS, an Egyptian government agency responsible for approving some types of off-campus research. CAPMAS issues are handled at AUC by the office of the University Counsellor. The IRB is not in a position to offer any opinion on CAPMAS issues, and takes no responsibility for obtaining CAPMAS approval.
This approval is valid for only one year. In case you have not finished data collection within a year, you need to apply for an extension.



CAPMAS Approval

جمهورية مصر العربية

الجهاز المركزى للتعبئة العامة والإحصاء

قرار رئيس الجهاز المركزي للتعبئة العامة والإحصاء

بالتفويض رقم (٥٢٤) لسنة ٢٠٢٢

فى شأن قيام الباحثة / دينا رفاعى محمد محمد على – المسجلة لدرجة الماجستير/ كلية الشئون الدولية والسياسات العامة قسم الصحافة والإعلام / الجامعة الأمريكية بالقاهرة - بإجراء دراسة ميدانية بعنوان: (تحليل وعي مستخدمى منصات التواصل الاجتماعى لسياسات الخصوصية والتعبير عن الرأي وإحتمالية مقاومة هذه السياسات من قبل المستخدمين).

رئيس الجهاز

- بعد الإطلاع على القرار الجمهوري رقم (٢٩١٥) لسنة ١٩٦٤بشان إنشاء الجهاز المركزى للتعبئة العامة والإحصاء.
- وعلى قرار رئيس الجهاز رقم (٢٣١) لسنة ١٩٦٨في شأن إجراء الإحصاءات والتعدادات والاستفتاءات والاستقصاءات.
- وعلي قرار رئيس الجهاز رقم (١٣١٤) لسنه ٢٠٠٧ بشأن التفويض في بعض الاختصاصات.
- وعلي قرار رئيس الجهاز رقم (١٥٥٢) لسنه ٢٠٢١ بشأن التفويض في بعض الاختصاصات.
- وعلى كتاب الجامعة الأمريكية بالقاهرة - الوارد للجهاز في ٤/١٢ /٢٠٢٢.

قـــــرر

مادة ١: تقوم الباحثة / دينا رفاعى محمد محمد على – المسجلة لدرجة الماجستير/ كلية الشئون الدولية والسياسات العامة قسم الصحافة والإعلام / الجامعة الأمريكية بالقاهرة - بإجراء الدراسة الميدانية المشار اليها عالية.

مادة ٢: تجرى الدراسة على عينة حجمها (٦٠٠) ستمائة مفردة من مستخدمى مواقع التواصل الاجتماعى مثل (الفيس بوك - تويتر انستجرام – وات ساب) بالفئة العمرية من (١٨ : ٧٠ سنة) .

مادة٣: تجمع البيانات اللازمة لهذه الدراسة بموجب الاستماره المعدة لذلك باللغتين العربية والأنجليزية وعدد صفحاتها سبع صفحات وتطبق "الكترونيا" معتمدة كل منهما بخاتم الجهاز المركزي للتعبئة العامة والإحصاء.

مادة ٤: يراعى موافقة مفردات العينة – وسرية البيانات الفردية طبقا لقانون الجهاز رقم (٣٥) لسنة ١٩٦٠ والمعدل بالقانون رقم (٢٨) لسنة ١٩٨٢ وعدم استخدام البيانات التي يتم جمعها لأغراض أخري غيرأغراض هذه الدراسة.

مادة ٥: يجري العمل الميداني خلال ثلاثة أشهر من تاريخ صدور هذا القرار .

مادة ٦: يوافى الجهاز المركزى للتعبئة العامة والإحصاء بنسخة من النتائج النهائية كاملة لهذه الدراسة.

مادة٧ : تلتزم الباحثة / دينا رفاعى محمد محمد على - بإبلاغ مديرية الأمن بمحافظة القاهرة - بصورة من هذا القرار وقبل البدء في التنفيذ مرفقا بها بيانات القائمين بالدراسة (الاسم – الرقم القومى – تاريخ بدء وانتهاء تنفيذ الدراسة)

مادة ٨: ينفذ هذا القرار من تاريخ صدور هذا القرار.

صدر في: ١٤/ ٤ / ٢٠٢٢

محمد إبراهيم بخيت
مدير عام الإدارة العامة للامن