T.R.
USKUDAR UNIVERSITY
INSTITUTE OF SCIENCE

MASTER'S DEGREE PROGRAM OF CYBER SECURITY

MASTER'S DEGREE THESIS

SOCIAL MEDIA REGULATIONS IN CYBER SECURITY

USAMA AHMAD MUGHAL

Thesis Supervisor
PROF. DR. SALIM JIBRIN DANBATTA

ISTANBUL-2024

ABSTRACT

SOCIAL MEDIA REGULATIONS IN CYBERSECURITY

In an era characterized by the pervasive integration of social media into daily life, the interconnection between cybersecurity and the regulatory landscape has become a crucial subject of investigation. The goal of this study is to perform a thorough examination of current regulations, industry practices, and conducting case studies to examine the reciprocal influence of social media and cybersecurity, and a review of the literature to investigates the efficacy of existing social media regulations in safeguarding against cyber threats, with a particular focus on data breaches, identity theft, and malicious activities. In this study, the research is classified as qualitative, focusing on current regulatory frameworks and an examination of notable cybersecurity incidents. Employing a systematic literature review methodology, the study aimed to gather, evaluate, and synthesize existing literature to gain insights into the nature and extent of cybersecurity challenges in social media. Conclusion and findings from the study will be helpful to social media users, groups, corporations, financial institutions, and regular individuals. This study provides a relevant investigation of the complex correlation between the regulation of social media and cybersecurity, providing valuable insights for policymakers, practitioners and researchers navigating the complex intersection of digital communication and online security.

Keywords: Cybersecurity; Laws; Cyber safety; Regulations; Social media; Vulnerability

ÖZET

Sosyal medyanın günlük yaşama yaygın entegrasyonu ile karakterize edilen bir dönemde, siber güvenlik ile düzenleyici çerçeve arasındaki etkileşim, araştırmanın kritik bir konusu haline gelmiştir. Bu çalışmanın amacı, mevcut düzenlemeleri, endüstri uygulamalarını derinlemesine incelemek ve sosyal medyanın siber güvenlik üzerindeki karşılıklı etkisini incelemek için vaka analizleri yaparak, mevcut sosyal medya düzenlemelerinin siber tehditlere karşı koruma sağlama etkinliğini incelemektir; bu özellikle veri ihlalleri, kimlik hırsızlığı ve kötü niyetli faaliyetlere odaklanır. Bu çalışmada, araştırma nitel olarak sınıflandırılmış olup, mevcut düzenleyici çerçevelere ve dikkate değer siber güvenlik olaylarının incelenmesine odaklanmaktadır. Sistematik bir literatür tarama metodolojisi kullanarak, çalışma, sosyal medyadaki siber güvenlik zorluklarının doğasını ve kapsamını anlamak için mevcut literatürü toplamayı, değerlendirmeyi ve sentezlemeyi amaçlamaktadır. Çalışmanın sonuçları ve bulguları, sosyal medya kullanıcıları, gruplar, şirketler, finans kurumları ve sıradan bireyler için faydalı olacaktır. Bu çalışma, sosyal medyanın düzenlenmesi ile siber güvenlik arasındaki karmaşık ilişkinin uygun bir incelemesini sunar; dijital iletişim ve çevrimiçi güvenliğin karmaşık kesişiminde gezinen politika yapıcılar, uygulayıcılar ve araştırmacılar için değerli içgörüler sunmaktadır.

Anahtar Kelimeler: Siber Güvenlik; Siber Güvenlik; Sosyal Medya; Düzenlemeler; Zafiyet; Yasalar

THANKS TO

In the name of Allah, the Most Generous, the Most Merciful. A lot of love for our beloved Holy Prophet MUHAMMAD (S.A.W), his guidance always helps us to get the right path.

The unending prayers and support of my parents are also, I gladly proclaim, the success indicators of my thesis.

This thesis would not have been possible without my supervisor's help, support, and guidance. I am very thankful and appreciate Prof. Dr. Salim Jibrin Danbatta, my supervisor. For always pushing me and showing me the way. He helped me every step of the way as I wrote my thesis.

I also want to thank my Honorable adviser Prof. Dr. Ahmet Senol for his managerial abilities, which have made it much easier for me to split my work up into manageable chunks and complete it. Moreover, He also helps me regarding the topic selection for thesis and any technical help needed.

I also want to thank the school staff and office workers in the Computer Information System Department for their hard work and dedication.

Finally, I want to thank my Father, Prof. Muhammad Munir Mughal and sisters, Warda, Sidra and Sumra for all the help and support they have given me. And also I want to thank my brother, Zaid Ahmed for all the help he gave me from the start of my studies to the end. Thank you all for all the support and motivation you've given me. I wouldn't be here without your help along the way, and I couldn't have written this thesis without you.

To my parents…

FORM OF DECLARATION

I hereby certify that I obtained all data and materials for this study within the parameters of academic standards, that I presented all visual, auditory, and written information and findings in accordance with scientific ethics, that I did not falsify the data I used, that I cited the sources I used in accordance with scientific norms, and that my thesis was original, with the exception of the cases cited, produced by me and written in accordance with the Üsküdar University Thesis Writing Guide.

10/05/2024

Usama Ahmad Mughal

Signature

CONTENTS

INDEX OF FIGURES

1. INTRODUCTION

The backdrop and problem of the study are presented in this chapter, also motivation for this work also included in this work, followed by the goal, importance, and restrictions of the study, as well as a summary of the research.

1.1. Preamble

There is a growing prevalence of privacy and security problems on social media platforms on a daily basis. On these platforms, hackers are actively seeking any information that might be used to launch an attack against a person. Hackers are motivated to acquire individuals' pet names, birth dates, account numbers, bank names, and other personal details that might be exploited to their disadvantage. In addition, they seek data that can be used to address any undisclosed inquiries that an individual may have established on their accounts. The assault will be considered successful if, for example, an individual publishes an anonymous inquiry requesting the identity of their pet animal, and the cyber attackers manage to obtain this data from their social media profile.

However, people on social media must confront the fact that their private data is readily available to their social media platforms for commercial purposes or can be sold to third parties. In order to prevent consequences, they are resorting to ineffective strategies to achieve their goal. Facebook and other social media platforms have faced allegations of privacy violations and have been legally convicted.

1.2. Overview of Cybersecurity Regulations

Directives known as cyber security regulations safeguard online systems and information technology. The purpose of these regulations is to restrict organizations' ability to safeguard their computers and data against cyber threats, including denial of service (DOS) attacks, worm and virus attacks, unauthorized access (e.g., online theft of intellectual property), control system attacks, and theft of confidential information. These regulations is/are not limited to/for just these types of directives. There is an increase in awareness regarding the spread of numerous strategies that are utilized by these hackers. (The Cybersecurity Regulation, 2021, Wikipedia)

The activation of firewalls, the installation of anti-virus software, the implementation of malware detection, prevention system, encryptions, and the development of login and passwords and two factor verification are examples of cyber security procedures. In an effort to stimulate advances in cyber security, there have been a variety of ways made to improve cyber security by the use of regulations and cooperative efforts with the Government. Banking and industry regulators have recognized the grave threat that cyber security poses and have initiated or plan to initiate the incorporation of cyber

security assessments into regulatory examinations. This is because cyber security poses a particularly significant threat.

1.3. Overview of privacy concerns

As a result of technological advancements, the amount and availability of information that is transmitted and stored via the internet have both grown. As a consequence, the role of cyber security has increased exceptionally among individuals and corporations. Violation of data means that the person might lose money, reputation and even be liable to a lawsuit if personal information is accessed illegally. A number of policies have been put into place so as to ensure privacy with the reliability of critical data in order to address these issues. As boundaries fade away, the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS) and General Data Protection Regulation (GDPR) are three legislative frameworks developed to protect delicate information as well as to negate data breaches.

The effectiveness of these limitations in achieving their aims is a critical arguing point in academic literature. The implementation of these policies has always been successful in establishing standards and raising awareness of cyber security but there are still issues regarding the execution of the policy. This work will aim at analyzing the effectiveness of such policies in safeguarding sensitive information and reducing data breaches, as well as identifying their limitations and shortcomings.

1.4. Problem Statement

To analyze the effects and security risks faced by social media users, together with possible ways to help in their evasion. As of now, people are using social networks and they have huge problems with privacy.

Social media is a new form of communication that undoubtedly brought about an all-around change in the ways information was being exchanged as it has provided us with a less time and cost consuming means of communicating. Social media's increased popularity and varied users base have prompted new challenges (Almarabeh & Sulieman, 2019). The accessibility of the internet service has led to a significant usage of social media and the sharing of information in recent years. The increasing number of individuals registering for social networking platforms such as Facebook, Snapchat, LinkedIn, and Instagram can be attributed to the progress in internet technology, enhanced availability of online information services, and the convenience of global communication. Social media platforms facilitate the creation of user profiles, initiation of conversations, and establishment of connections between users. People often neglect to assess the authenticity of the evidence as they tend to be the initial inquirers (Rahman, et al. 2020).

Social media is becoming increasingly corrupted, prioritizing profit over promoting users' optimal interactions. Several businesses are competing for the profitable digital marketing market share before it becomes exhausted. Undoubtedly, social media is the most convenient platform to access readily available data from the general public without extensive searching, and companies are maximizing their profits from their customers on these platforms. Another organization prioritizes the collection and utilization of user's personal information. This category contains both attackers and government agencies. Scammers, spammers, hackers, and social engineers represent some instances of malicious individuals. Some individuals persist in monitoring individuals' activities, posts, and public disclosures on many social platforms. Social-media platforms provide an abundance of data on individuals, making it exceptionally convenient for social engineers to access. They utilize this data to trick individuals into believing that they are genuine bank personnel, government officials, or employees of other organizations. These criminals target only people who are innocent due to social media platforms' focus on maintaining public access to user data. In addition, there have been claims that certain nations deliberately engaged in online monitoring of their citizens. They reportedly exert pressure on the platforms to disclose communications and other confidential user data. Additionally, it is reported that they possess an exceptional team of skilled hackers who exclusively access user accounts when it seems necessary. They implement this measure to prevent the local community from terrorist attacks.

The main reason for the current research is the substantial rise in the number of people who have been targeted and affected by individual cyberattacks. Cybercrime and virus attacks on social networking platforms compromise the privacy and information of users. The vulnerability of the human element in online social networks stems from the absence of adequate cybersecurity skills among individuals. Many individuals lack comprehension of cybersecurity, cybercrime, and effective strategies for protecting themselves against such forms of electronic warfare.

1.5. Aim Of the study

The main goal of this study is to look at a lot of literature to learn about the laws and rules that apply to social media in the area of cybersecurity (Nadia, et al. 2023). Its objective is to tackle the rules and security concerns now faced by social media users. Additionally, it aims to provide feasible solutions that can be put into practice, together with the necessary legal measures that governments should adopt and the responsible actions that social media companies should take on behalf of susceptible social media users. The objective is to empower social media users by providing them with knowledge about rules, regulations, vulnerabilities, and strategies to mitigate risks.

1.6. Significance of the study

This research has different applications. This article provides a concise overview of the security and regulatory concerns that consumers encounter when utilizing online services. Regarding concerns about privacy, it examines both the issues arising from social media corporations and those arising from users' careless disclosure of information.

Nowadays social networking sites provide individuals with access to personal information, financial data, news, medical data, e-commerce, and other fundamental aspects of daily life. The research holds significance as it furnishes facts and suggestions regarding social media security and explores regulatory measures. Disseminating information on cybercrime, cybersecurity, and cyberthreats that peoples on social media encounter via social media platforms is crucial. Although there is a lack of similar research on this subject, The implications of this study's findings extend to individuals who utilize social media. The findings can be advantageous to a broad range of individuals, as well as employees, companies, students and their parents alike. By providing users with information regarding the regulations of social media, they can interact with these platforms in a more secure and regulated way (Robinson RJ, 2023).

1.7. Limitations of the Study

The limitations of the study have been defined as follows:

The present study includes four databases, namely Science Direct, Web of Science, Scopus, and IEEE Explore.

The research proved entirely about the function of cybersecurity legislation on social media platforms.

• The articles included are limited to the period from 2013 to 2023.

• This study exclusively includes papers that are specifically focused on reviewing an area of study.

• The assessment of research quality is limited.

• Numerous evaluations lacked adequate abstracts of the involved studies.

1.8. Overview of the Study

To help readers understand the complete thesis, the study outlines five chapters.

Chapter 1: Give some background on the history of the study and an overview of regulations and legislations of social media in cyber security. After a summary of the research, the researchers explained what the main problems are, how important it is, the objective of this study, and what are the limitations of it.

Chapter 2: Presents relevant research and introduces a theoretical framework wherein numerous social media cybersecurity regulatory issues as well as some of the platform's characteristics and the corresponding concerns were examined.

Chapter 3: Provides a thorough explanation of the particular study, research process, quality assessment, selection criteria, descriptive analysis, and data extraction, that were used to methodically acquire, analyses, and choose relevant publications using the PRISMA framework.

Chapter 4: Results from the study's research questions are presented in Chapter 4, which gives the study's interpretation and description. Findings for each pertinent piece of literature are scheduled for all records in accordance with PRISMA principles. The elements are then shown and tabulated in a tabular manner separately for each research topic, followed by a discussion of the thesis.

Chapter 5: Includes discussions about document analysis and the debate over the findings and highlights of the critical need for improved cybersecurity rules and regulations in social media platforms.

Chapter 6: Includes the whole research study's conclusion as well as suggestions for the thesis, concepts, and future studies.

2. Theoretical Concept

This chapter also gives the theoretical framework along with focus on earlier studies that are Applicable to current research that is social media and cybersecurity.

2.1. Cybersecurity

Cybersecurity refers to the act of Protecting networks and their systems and softwares from cyberattacks. Normally, these targets the goal of gaining unauthorized access, modifying and breaching confidential data, disrupting regular corporate operations. Cybersecurity refers to a collection of methods deployed to safeguard computers, networks, softwares and information from unwanted access, harm and invasion. The prevention of malicious softwares (malware), The prevention of illegal access to computer systems and the protection of data from theft. Furthermore it involves the creation of safe software and ensuring the timely updating of systems, providing education to users regarding security practices and conducting regular vulnerability assessments. Confirming cyber security is crucial for businesses, organizations and individuals in safeguarding their data and systems from Malicious attacks.

The reason behind its importance is that it contains necessary and crucial details like personal information, financial data and trade secrets which are very sensitive and even takes step of preventing any kind of Disturbance. A strong cyber security will build trust with customers and protect online transactions as well as interactions with stakeholders.

2.1.1. Cybersecurity Types

Cybersecurity is like a protective shield that includes various security measures to safeguard of digital world. Its about keeping our computers and valuable data safe from harm. Within cybersecurity, there are different guardians that work Relentlessly to defend against threats:

Network Security:

Firewalls:- are used to monitor and control the flow of network data.

Intrusion Prevention Systems (IPS):- are used for Detecting and preventing unauthorized access.

Endpoint Security:

Antivirus Softwares:- are used for Protecting individual devices from malicious viruses and other threats.

Application Security:

Web Application Security:- are used to ensure the protection of web applications against security risks and weakness.

Cloud Security:

Cloud Access Security Brokers :- are used to Monitor and overseeing security rules for data that are saved in the cloud.

Data Security:

Encryption:- In this process we safeguard sensitive data by converting it into a coded format that can only be decoded with the correct secret encryption key.

Physical Security:- Implementing the steps to safeguard physical infrastructures such as servers and data centers for unwanted access and harm.

Wireless Security:- Implementation of security measures for wireless networks just like Wi-Fi to protect against unauthorized access.

To provide total defense against different threats in the cyberspace, usually these cyber security measures are used.

2.1.2. Cybersecurity Threats

Cybersecurity threats are in a constant state of Variability as technology grows more Advanced and hackers develop new methods to exploit vulnerabilities. below are mentioned some common threats in cybersecurity:

1. **Malware:**

   Viruses: It refers to a type of malicious software program designed to replicate itself and spread from one computer to another computer.

   Trojans: Trojans are a type of malicious software program that pretends as legitimate software to deceive users into downloading and installing them.

   Ransomware: Ransomware is a type of malicious software designed to block access to a computer system or files until a sum of money, ransom is paid.

   Spyware: they are designed to secretly monitor and gather information from a users computer without their knowledge.

2. **Phishing:-** Phishing refers to the act of using fake emails, texts and websites that replicate reliable sources in order to deceive individuals into Sharing confidential information.
3. **Denial of Service Attacks:-** Distributed Denial of Service is the act of Overloading a system, network or a website with an excessive amount of traffic in order to Make it unreachable to users.
4. **Man in the Middle Attacks:-** Man in the Middle is a type of cyber attack where a malicious actor intercept and alters communication between two parties without their knowledge.
5. **Cross-Site Scripting :-** Cross-Site Scripting (XSS) is like a sneaky trick played on websites. It happens when hacker inject harmful code, like viruses into web pages. When you visit those infected pages bad code runs on your computer letting the attackers steal your information, take control of your accounts.
6. **Insider Threats:-** The insider threat is the term used to refer to any intentional or unintentional behaviors of organization's employees, contractors or anyone else that can lead to a breach of security measures.
7. **Credential Theft:-** Credential theft when someone steals your usernames and passwords to access accounts and sensitive information.
8. **Social Engineering:-** Social engineering is manipulation to deceive individuals into divulging confidential information or performing actions beneficial to the attacker. It exploits human psychology, often through impersonation or persuasion, to bypass security measures and gain unauthorized access to systems or data.

To keep safe from these threats both companies and people needs to follow a mix of rules and learn about staying secure. This means updating software regularly, setting up firewalls and using antivirus programs to protect our computers and personal information.

2.2. Social Media

The digital tools and technologies that make up social media enable people to create, exchange and share content within online networks. These platforms are designed to enhance social interactions by enabling individuals to establish connections, communicate with others and exchange information on the internet.

Service	Accounts
Facebook	3.69 Billion
Instagram	2.5 Billion
WhatsApp	2.8 Billion
Twitter	354 Million
Snapchat	525 Million
LinkedIn	930 Million
YouTube	2.7 Billion
TikTok	1.67 Billion

Figure 1: Leading social media services worldwide by active user accounts (Source “Google”)

On a cybersecurity level various issues and dangers through social media arise as a result of the huge quantities of personal informatio. The interactive nature of these platforms and their potential for malicious activities.

Below are some key cybersecurity considerations:

- Data Privacy and Protection
- Phishing and Social Engineering
- Account Security
- Malware Distribution
- Impersonation and Fake Accounts
- Employee Training
- Regulatory Compliance
- User Education
- Data Protection Regulations
- Information Sharing

The collaboration of social media platforms with cybersecurity communities can enable them to share threat intelligence and enhance security bodies. For users as well as those companies that run social media platforms, these points is fundamental in order to build a secure online environment. Continuous awareness and the taking of proactive steps are crucially important.

2.2.1. Social Media Types

In social media there is a wide variety of platforms that are meant to facilitate different kinds of communication, interaction and sharing of information:

1. **Social Networking Sites:**

   Social networking platforms facilitate users to establish connections with friends, family, and coworkers, exchange updates, and establish a network of contacts.

   Examples: Facebook, LinkedIn, Myspace (historical).

2. **Microblogging Platforms:**

   Includes Services in which users share short, concise updates, often in the form of text, links and multimedia content.

   Examples: Twitter, Tumblr.

3. **Photo-Sharing Platforms:**

   These Platforms are focused on sharing and discovering photos and visual contents.

   Examples: Instagram, Snapchat, Pinterest.

4. **Video-Sharing Platforms:**

   Those Platforms where users can upload/share and discover videos.

   Examples: YouTube, TikTok, Vimeo.

5. **Professional Networking Platforms:**

   Platforms that are used for professional networking, Job searching and Career Development.

   Examples: LinkedIn, Xing.

6. **Discussion Forums and Message Boards:**

   They are Platforms where users participate in discussions, ask questions and share information within specific interest.

   Examples: Reddit, Quora.

7. **Blogging Platforms:**

   Used for creating and publishing blog posts and articles.

   Examples: WordPress, Blogger, Medium.

8. **Live Streaming Platforms:**

   There users are allow to broadcast live video content, used for gaming and personal interest.

   Examples: Twitch, Facebook Live, YouTube Live.

9. **Location-Based Social Networks:**

   Platforms that focus on sharing location-based information, such as check-ins and recommendations.

   Examples: Foursquare, Swarm.

10. **Dating Apps and Platforms:**

    Services designed to connect individuals for dating or romantic relationships.

    Examples: Tinder, Bumble.

11. **Ephemeral Content Platforms:**

    Platforms where content, such as photos or videos, disappears after a short period, fostering a sense of impermanence.

    Examples: Snapchat, Instagram Stories.

These are just a few examples of how social media is changing. New platforms and trends are always coming out.

2.2.2. Social media challenges and their Response:

Creating effective regulations for social media from a cybersecurity point of view can be difficult due to the changing nature of these platforms as evaluation of cyber threats and the need to balance security with user privacy and freedom. Here are some challenges that a cybersecurity expert faces while drafting regulations for social media:

2.2.2.1. Privacy Dilemma:

Challenge: Balance the need for very strong cybersecurity measures with user privacy concerns can be difficult. keeping the right balance is critical to building trust while assuring security.

Approach: Develop some regulations that clearly tells how user data should be handled, with transparency, informed consent and the right to control user's personal information.

2.2.2.2. Global and Cross-Border Nature:

Challenge: Social media are now operated globally so it is difficult to create regulations that are universally applicable and enforceable in different jurisdictions.

Approach: Encourage and motivate international collaboration and development of global standards are needed, also considering mechanisms for crossborder co-operation on issues of cybersecurity.

2.2.2.3. Dynamic Threat Landscape:

Challenge: Cybersecurity threats are constantly increasing and regulations must be flexible to adapt new and growing challenges.

Approach: Need to develop regulations that require monitoring, regular assessments of risk and response to growing threats with the flexibility to update security measures.

2.2.2.4. User Authentication and Identity Verification:

Challenge: Problem in Protecting users authentication while avoiding identity verification methods that are unwanted.

Approach: Develop Regulations that encourage the strong authentication methods without compromising the privacy of user and promote the use of identity verification measures with effective and respectful to user rights.

2.2.2.5. Content Moderation and Censorship Concerns:

Challenge: facing concerns that are related to content moderation and hate speech and potential abuse of regulatory powers for censorship.

Approach: Develop clear cut guidelines for the moderation of content, encouraging transparency, due process and also user appeals.

2.2.2.6. Incident Response and Reporting:

Challenge: Establishing regulations that gives direction of effective incident response plans and timely reporting of incidents in cybersecurity.

Approach: Develop regulations that shape specific incident response requirements, reporting timelines and consequences for non-compliance.

2.2.2.7. Regulatory Compliance and Enforcement:

Challenge: Making sure that social media platforms must comply with cybersecurity regulations and faces consequences for non-compliance.

Approach: Need to establish a regulatory framework with regular audits, penalties for those with non-compliance and the collaboration with law enforcement agencies where it is necessary.

2.2.2.8. Public-Private Collaboration:

Challenge: Promote collaboration between regulatory bodies, social media and cybersecurity experts to keep track of challenges together.

Approach: To Develop regulations that encourages information sharing and collaboration. Facilitate forums for regular communication between stakeholders.

2.2.2.9. Education and Awareness:

Challenge: Encouraging awareness of the cybersecurity and education to users and administrators of Social media platforms.

Approach: TO Include arrangements in regulations that provides cybersecurity awareness campaigns and training programs with resources for users and platform staff.

2.2.2.10. Technology Integration:

Challenge: It is important to keep regulations up-to-date in response to the rapid progress made by technology such as virtual reality, augmented reality and artificial intelligence.

Approach: Create guidelines that consider upcoming technologies, promote cautious progress and integration and integrate assessments of technology at regular intervals.

Creating Good cybersecurity regulations for social media requires a deep understanding of the platform dynamics, their user behaviors and the increasing cyber threats.

2.3 Social Media Regulations:

Social media regulations are the rules, guidelines and policies established by government regulatory bodies and the platforms themselves to govern the use and conduct on social media. These regulations are design to address various concerns that is including privacy security, misinformation, hate speech and much more. The specific regulations can vary significantly from one country to another, Taking into consideration of cultural, legal and political variances. The benefits of social media are clear.

However more and more evidence is surfacing causing the increase in concern about the harmful effects of it. The analyzer of social media argues that the content found on these platforms potentially cause harm in several manners. They can be as a tool for spreading hateful harassment. They have the ability to harm public health by spreading inaccurate information. Social media platforms have the ability to shape the perceptions of young individuals, leading them to adopt unfavorable self-perceptions and promoting addictive behavior that diverts their attention from physical activities.

Although freedom of expression is highly safeguarded, the Supreme Court has granted the government the authority to restrict or penalize specific forms of speech. Speech that is subject to prohibition encompasses obscenity, slander/libel, and the act of encouraging impending illegal action.

Furthermore, the Court has granted permission for certain restrictions on the timing, location, and method of communication.

In 1996, prior to the widespread use of social media, the Communications Decency Act had been passed by Congress. Section 230, grants the social media platforms authority to remove any speech at their judgment without facing legal consequences. However, there is one notable exception: the corporations bear the responsibility for addressing copyright violation allegations and instances of child sex trafficking that occur on their platforms. Section 230 grants companies the authority to remove speech at their discretion without facing legal consequences for violating a user's rights (sustainability, n.d.).

Companies put artificial intelligence and good number of workers and external firms to see and delete harmful information and accounts that are bogus.

Social media regulations involve developing rules and policy/policies to make sure the correct use of the platforms and maintain a positive good environment. The exact regulations for a social media site may be different due to its nature and jurisdiction. Here are mentioned some of the key areas to consider when developing regulations for a social media sites:

2.3.1. Terms of Service (ToS) and User Agreement:

It Clearly defines the terms of service and user agreement that all the users must agree when creating their account. Outline acceptable behavior, content policies and consequences for violations.

2.3.2. Privacy and Data Protection:

Clearly communicate how user data is collected/stored and used. Must Comply with relevant data protection laws and provides users with transparency about data practices including options for consent and control.

2.3.3. User Authentication and Verification:

To establish system for user authentication to block fake accounts and identity theft. Must consider identity verification processes for users wish to increase their credibility on the platform.

2.3.4. Content Moderation Policies:

Defined content moderation policies in place to address issues like hate speech, harassment & violence and the misinformation. Clearly communicate which types of contents are prohibited and establish reporting system for users to flag/report inappropriate content.

2.3.5. Community Guidelines:

To develop good community guidelines that outline expected behavior and values on the platform while discouraging harmful activities.

2.3.6. Account Security:

To Implement set in place the security protocols to safeguard user accounts including strong password requirements, multi factor authentication process and the account recovery options. Inform users about best practices for maintaining the security of account.

2.3.7. Child Online Protection:

To setup measures to protect children using the platform, is in compliance with relevant laws. Implementation of age verification system and creating a safe and secure environment for minors.

2.3.8. Cybersecurity Measures:

To execute Good and effective cybersecurity protocols to safeguard the platform against new cyber threats. This comprises of frequent audits of security and encryption protocols and safety measures to minimize the risk of data breaches.

2.3.9. Advertising and Sponsored Content:

Outline policies regarding advertising and sponsored content on the Social media platforms. To ensure transparency in advertising practices and do compliance with regulations such as disclosure requirements.

2.3.10. Reporting Mechanisms and Customer Support:

To Create a good userfriendly reporting system for the violations of community guidelines. and to Provide customer support to address user concerns and inquiries related to the platform.

2.3.11. Accessibility:

To ensure that the system is easily usable for the individuals with disabilities and to Comply with accessibility requirements in order to provide equal access for individuals with various requirements.

2.3.12. Regular Compliance Audits:

To Conduct the regular audits to assess compliance with regulations in place. Updating of policies as needed to adapt to growing user needs, legal requirements.

2.3.13. Communication and Transparency:

To Communicate changes to policies and updates with important information to users transparently. By keeping users informed about the platforms practices and developments ahead. It's essential to stay informed about evolving legal and regulatory landscapes, as the regulatory environment for social media is subject to change.

2.4. International Regulations and Laws Regarding Cybersecurity

Countries have addressed cybercrime by implementing legislation and regulations to oversee the use of data in areas such as communication, finance, healthcare, and other digital transactions. Historically, cybercrime was limited to copyright violations and software piracy. Nevertheless, there has been a rise in serious criminal acts that necessitate the establishment of specific legislation in all domains and across nations to reduce the rise of such crimes (Ellis and Mohan, 2019). Furthermore, the task of enacting legislation that can effectively adapt to the swift advancements in technology has become increasingly challenging. Furthermore, there exists a correlation between these laws and human rights, given that countries employ diverse strategies to oversee the digital activities of internet users, so violating upon privacy in certain instances. Countries are examining this matter in order to establish a balance that safeguards both human rights and state sovereignty, ensuring the protection of their population and national security. Hence, it is essential for lawmakers, regulators, technologists, and scientists with a deep understanding of technology to engage in the exchange of experiences and information (Brivat, 2017).

In 2016, the General Data Protection Regulation (GDPR) was introduced by the European Union as a measure to address the increasing occurrence of cybercrime. This legislative framework establishes guiding principle for the handling, transfer, and processing of personal data for individual's resident in European Union nations and the European Economic Area. The GDPR was officially adopted in 2018. These requirements are applicable to websites that are accessed or utilized by individuals who are inhabitants of the European Union, irrespective of whether these websites are exclusively intended for EU residents or are accessible to individuals from other parts of the world. The General Data Protection Regulation (GDPR) consolidates and standardizes all legislation pertaining to data protection for European Union (EU) people, simplifying compliance for enterprises and websites. (Kosseff, 2019).

PIPEDA, like GDPR, brings together all the rules about personal data and gives people the right to see their own personal data held by companies, ascertain the accountable party for this information, and verify its accuracy. The Canadian government announced in 2017, that it has achieved a level of data privacy comparable to that mandated by European Union legislation. This achievement enables the smooth and secure transfer of data between the European Union and Canada (Kosseff, 2019).

In the United States (U.S.), there are numerous laws and regulations that pertain to the domain of cybersecurity, although only a small number of them explicitly reference cybersecurity by its term. The Federal Trade Commission (FTC) is the governing body responsible for overseeing cybersecurity legislation, encompassing areas such as data security, hacking, electronic and privacy surveillance, and the disclosure of data breaches. (Kosseff, 2019).

2.5. Regulation of Social Media and Cybersecurity in Saudi Arabia

The cybersecurity baseline criteria for Saudi government organizations were introduced by the National Cybersecurity Authority of Saudi Arabia in 2018. This framework includes 114 cybersecurity controls aligned with national and international standards. These controls are divided into 5 categories mainly: first governance, second cybersecurity defense, third cybersecurity resilience, forth third-party and cloud computing cybersecurity, and last industrial control systems (NCA, 2020).

The primary purpose of these controls is to establish a baseline for essential cybersecurity measures, drawing from industry standards and practices at best. They aim to mitigate cyber risks to organizations' IT assets, addressing internal as well as external threats. In order to follow the laws and rules that apply, the National Cybersecurity Authority has set up governance requirements that require the formulation and implementation of a cybersecurity plan. The Entity Control Center (ECC) outlines the necessary personnel, processes, and procedures for comprehensive cybersecurity (Alsmadi and Zarour, 2018).

Within the realm of cybersecurity governance, the strategy and management encompass the establishment of policies, procedures, and communication of cybersecurity standards based on regulatory business requirements. Clearly defined tasks and responsibilities in cybersecurity and risk management are organized to protect the entity's information and technology assets.

It is essential that the entity's project methods and procedures incorporate cybersecurity standards to ensure protection the confidentiality and integrity of technological and informational assets. Compliance with legislation, regulations, and standards pertaining to cybersecurity is regarded as an essential component of cybersecurity governance (National Cybersecurity Authority, 2020).

Regular cybersecurity checks and audits are essential, ensuring compliance with cybersecurity risks and standards related to social media and end users. The National Cybersecurity Authority (2020) recommends the development and periodic implementation of a program aimed at enhancing cybersecurity knowledge. This program should be disseminated through various channels to promote a positive cybersecurity culture.

2.6. Cybersecurity and social media Regulation in Pakistan

The percentage of the users using the internet & social media in Pakistan are increasing rapidly.
In recent past years, Pakistan has made some critical changes to improve its cyber security. In 2019 the Ministry of Information Technology and Telecommunications launched the National Response Center for Cyber Crimes. This center has been involved in increasing awareness about cyber threats and co-ordinating between law enforcement and other relevant agencies on cyber crime issues. This center is also developing training materials for law enforcement officers and raises public awareness about cyber safety and security best practices. The government has also placed several laws to help protect against cyber crime.

In August 2020 The Prevention of Electronic Crimes Act (P.E.C.A) recieved approval by the National Assembly which criminalized several of the activities including hacking, fraud, intellectual property rights violation and identity theft. The government issued guidelines for protecting the personal data of individuals, including measures to prevent unauthorized access and disclosure. Despite these workings, there are still other difficulties that must be resolved in order to establish a secure cyberspace in Pakistan. Adequate resources and personnel to be improved to investigate cyber threats and enforce cyber laws. Moreover there are areas for improvement in current legal frameworks that make it challenging to follow the latest cyber crime cases. Furthermore, the country's critical infrastructure remained vulnerable/easy to attack due to outdated technology and weak measures. Finally there is a need to develop Good policies and strategies that addresses both domestic and international threats. It is clear that Pakistan still face a range of cyber security challenges. By taking steps such as improving laws and regulations, strengthen protection measures and enhancing collaboration between relevant stakeholders the country can make progress toward achieving a safe and secure cyberspace for its citizens.

Threats	Domains
Surveillance	Social, E-commerce, environment, and political governance
User Profile	Actives and behavioral characteristics
Cyberstalking	Harassment and intimidation
Clickjacking	Press the link or like button, move cursors, use the camera and microphone
Location Privacy	Geotagging
Identity profile cloning	Creating a fake profile
Information Leakage	Health, infrastructure, operational, and intellectual property information
Fake profile Attacks	User information
De-anonymization	Health services, social media, and E-commerce trades
Inference Attacks	Prediction Sensitive, political, religious, and educational information

Figure 2: Modern threats and projected data attacks. (Source “Google”)

To address these challenges, effective policy measures that promote cyber security amongst organizations operating in Pakistan need to be established. There is a need to develop a comprehensive regulatory framework that will ensure the safety of digital systems and networks.

For Pakistan to be better protected from cyber threats, it must strengthen its legal framework on cyber security and increase investment into technological solutions that can defend networks from attack. The government needs more effective coordination between law enforcement agencies and tech companies to identify malicious actors online and take appropriate action against them.

To ensure an effective response against malicious online activities, Pakistan Telecommunication Authority (PTA) has blocked more than 800 websites hosting anti-state content since 2016. It has taken further proactive steps like setting up a 24/7 monitoring system for social media websites & networks.

The National Assembly of Pakistan has passed the Cyber Security Act, 2018, which aims to protect citizens from cybercrime by strengthening the legal framework and providing safeguards against cybercrimes. However, the effectiveness of the law is yet to be seen. By developing a culture of preparing for and protecting against future attacks, we can reduce the number and severity of incidents our society suffers in this digital age.

2.6.1. Improve Governance & Legislation:

The Government should/must implement very strict cyber security laws and regulations to protect the country from malicious activities. This process includes watching citizens data and imposing heavy penalties on cyber criminals and also protecting critical infrastructure.

2.6.2. Focus on Network Security:

Companies needs to increase their security investments and focus on updating their networks with the latest cybersecurity solutions. This strategy will/budgets, that will enable them to detect malicious activity more early and prevent significant data breaches.

2.6.3. Train Cyber Security Professionals:

The government should train peoples who work in cyber security to deal with growing number of risk.

2.7. Cybersecurity and social media Regulation in Turkey

Turkey has implemented certain cybersecurity measures and regulations related to social media. Nevertheless, this legislation may have undergone changes since that time, and it is crucial to authenticate the most up-to-date information from trustworthy sources. Here are some cybersecurity-related aspects that were relevant to social media regulations in Turkey.

All internet service providers in Turkey must register with the Information and Communication Technologies Authority (BTK). Social media firms are obligated to offer customers straightforward privacy settings and tools to manage their data.

The implementation of the Social Media Law in 2020 mandated that social media platforms must retain the user data of Turkish nationals inside the borders of Turkey. This measure was intended to enhance data security and give Turkish authorities more control over the protection of user information.

Social media networks with a daily user base above one million were required by legislation to designate a local representative in Turkey. This representative acts as the government authorities' point of contact, and their presence is seen as a way to facilitate cooperation in addressing cybersecurity concerns.

The law granted authorities the power to request the removal of content. From a cybersecurity perspective, this might have something to do with attempts to stop the spread of harmful or malicious content on social media sites.

The Information and Communication Technologies Authority was designated to oversee compliance with the Social Media Law. This includes ensuring that social media platforms adhere to cybersecurity measures and cooperate with Turkish authorities on issues related to online security.

In this study, my research is classified as qualitative potential research on regulations on social

Also in turkey Social media companies must provide users with the option to opt-out of targeted advertising and must not collect data for this purpose without explicit consent (Social media law, aysegulzengin, 2020).

3. MATERIAL AND METHOD

3.1. Sort of the Research

In this study, my research is classified as qualitative potential research on regulations on social media by cyber security. Qualitative research is conducted with the objective of understanding and gaining a deeper insight into the intricacies and nuances of the subject matter, this qualitative research will explore cyber security regulations and social media platforms, incorporating user perceptions, challenges facing the platforms, and adequacy of current regulatory frameworks.

This qualitative research sheds light on the complicated space of cybersecurity regulations on social media. It focuses on the necessity of user-centered regulations, platform flexibility, and global cooperation to respond to cybersecurity issues of the changing social media landscape.

This approach aims to provide a comprehensive and integrated understanding of the cybersecurity regulations encountered by social media platforms, highlighting possible gaps and providing insights into improving security measures and areas for improvement in current cybersecurity practices by systematically reviewing the literature. The results of this study will be introduced as a new contribution to the knowledge base on social media cybersecurity, emphasizing current challenges and potential solutions. The results will help to find significant areas of concern and will offer clues for the establishment of appropriate strategies and initiatives aimed at enhancing the cybersecurity practices on social media platforms.

3.1.1. Methodology

The qualitative research methods are most suitable for this study because they allow the researcher to gather a lot of information, which includes contextual data that is not only a numerical value (Hennink et al., 2020).

Sampling: The research targets purposive sampling of social media users, platform administrators, and cyber security experts.

3.1.2. Data Collection

1. **In-depth Discussions**: The researcher conducted a combination of semi-structured discussion, random discussion, and social media polls to understand the intricate perspectives of participants on their experiences, concerns, and opinions regarding social media regulations. This comprehensive approach provided a multifaceted understanding of the diverse viewpoints within the research area.

2. **Content Analysis**: Exploring official documents, policies and commentaries from social media platforms to determine their approaches towards cyber security regulations.

3.1.3. Themes and Findings

First User Perceptions:

According to our research almost 60% users raised issues of identity theft, data security, and the potential misappropriation of personal information. These users are mostly related to information technology area. The awareness of the cyber security risks is still widespread, but there are also doubts about the effectiveness of current regulation.

Then Trust in Platforms:

Cyber security measures perceived by users determine their trust in social media platforms. Others merely doubts about the platforms actions, while some believe in platforms' commitment to user safety.

Platform Challenges:

Social media platforms face the challenge of balancing user privacy with the need for data analytics to enhance user experience and targeted advertising.

Explain

Emerging Threats:

Social media platforms highlight challenges posed by emerging cyber security threats, including phishing attacks, deepfakes, and coordinated disinformation campaigns.

3.1.4. Effectiveness of Regulations

User Empowerment:

Some users express a desire for more control over their digital footprint and advocate for regulations that empower users to make informed choices about data sharing.

Platform Responsiveness:

The study identifies instances where platforms have adjusted policies in response to emerging cyber security threats, showcasing the adaptability of regulatory frameworks.

3.2. Collaboration Initiatives

Platforms are increasingly engaging in collaborative efforts with cyber security experts, governmental agencies, and non-profit organizations to strengthen their regulatory approaches.: Research Objective

With this study on cyber security rules for social media, the researchers hope to get a full picture of the complex situation where cyber security rules meet social media platforms. These comprise the three primary objectives of this research. First, the study wants to find out how social media users feel about cyber security and what worries them. It will focus on how many of them are conscious of risks such as data breach, identity theft and abuse of private information. The study seeks to determine how effective the current cyber security policies are in easing users' fears and offering trust to online environment by analysing what people think about them.

The second part of the research is aimed at uncovering the challenges social networking sites experience when trying to comply with cyber security regulations. That also includes looking at the thin red line these platforms have to run between protection of user privacy and user data monetization for better services. The cyber security threats such as phishing attacks, deep fakes, disinformation campaigns are constantly evolving. This study will focus on how these platforms are dealing with these issues through policy shifts and innovation.

Third, the research aims to determine the effectiveness of the existing cyber security regulations on social media sites. For this reason, it is focusing on how regulations influence user self-determination and whether the users perceive themselves as fully informed and in control of their online identity. Secondly, the study will consider how platforms react to different threats and examples of how regulatory frameworks have been adjusted to deal with new cyberspace malpractice. Further, a research effort at the international level is required to understand approaches to regulation and policy in different regions, as well as attempts at cooperation between government agencies, social media companies, and cyber-security experts.

Primarily, the purposes of this study are more than just a basic analysis of cyber security regulations on social media and to get into the detailed dynamics of how users perceive these rules, issues that may arise with these rules, as well as how effective they are overall in securing the cybersphere. In meeting such objectives, the study will generate valuable information that may influence future changes in cyber security laws to make a better and more user-oriented scene in the dynamic world of the Internet.

3.3. Search Strategy

The search strategy for this study involved a systematic and comprehensive approach to identifying relevant data on cybersecurity regulations on social media platforms.

Different search engines were used to gather data over the topic of my thesis. Like Google and also searched on academic databases like PubMed, IEEE Xplore, and other articles.

We looked for peer-reviewed academic journals that specialize in cyber security, law, or technology policy as well as recent articles discussing the legal and regulatory aspects of cyber security on social media.

To begin the search, acceptable keywords, and search terms such as "social media cyber security regulations," "online privacy laws," "data protection policies," "platform security standards" and similar terms were identified. Use of Synonyms and Variations to ensure we capture a broader range of relevant information "cyber security legislation" instead of just "regulations."

We used Boolean operators (AND, OR, NOT) to combine or exclude keywords for more precise searches. Like

"Social media cyber security regulations" AND "user privacy"

“data protection policies" OR "online security laws"

Explore official government websites, regulatory bodies, and organizations responsible for cyber security regulations.

Going through Case studies also give us real-life examples of how social media regulations have impacted cybersecurity. Industry reports from trusted sources, such as cybersecurity organizations and technology companies, were accessed to gather relevant information for the thesis.

3.4. Inclusion and Exclusion Criteria

In research, inclusion and exclusion criteria are established guidelines that define the characteristics or attributes that **must have (inclusion criteria)** or **lack (exclusion criteria)** to be eligible for taking part in a study.

In developing inclusion criteria for research on cybersecurity regulations on social media, certain key factors were considered to ensure a targeted and relevant study population. First, focused on including active social media users who engage in diverse online activities, such as posting, sharing, and commenting. Specified the age range to capture insights across different generations, and consider diverse demographics, including gender, ethnicity, and educational backgrounds. Geographical representation is crucial to obtaining a global viewpoint, and participants should consent to sharing

information for research purposes. Distinguish between different social media platforms and their users to analyze platform-specific nuances. It's beneficial to include individuals with legal or regulatory expertise related to cybersecurity to enrich the study's insights. Address privacy concerns by including participants with different levels of apprehension about online privacy. Furthermore, the literature primarily emphasized the need for cybersecurity policies that are relevant to each social media site. This criterion helped maintain a limited and concentrated scope for the review.

The other type of criteria was used to get rid of studies that didn't meet the criteria or didn't seem to be connected to the research goals. When crafting exclusion criteria for research on cybersecurity regulations on social media, I Began by excluding individuals below a certain age, ensuring that participants can provide mature insights. Excluded inactive social media users to concentrate on those actively engaged in online platforms. Excluded participants with minimal awareness of cybersecurity concerns to enhance the study's relevance. Language barriers were one of the main reasons for exclusion to ensure effective communication. Using criteria for what to include and what to leave out, the systematic literature review focused on relevant material that met the specific study goals. The review process was strict and methodical because it followed these standards. This made sure that the findings were real and reliable.

3.5. Data Extraction and Synthesis

In the last step of the study's PRISMA design, data from different studies are gathered, which includes gathering information and determining the response to each research question. Once all the papers used in the study were found, the relevant data from each one was carefully collected and calculated based on the research questions. The study extracted data from each paper pertaining to its purpose, publication date, key conclusion, and conducted technique. During this phase, the study eliminated other articles as they failed to address any research inquiries. The information was derived from the research inquiry, which focused on the type of cyberattack, factors contributing to susceptibility, methods of raising awareness about cybersecurity, and preventive measures. My research objectives were clearly defined, encompassing an extensive literature review to identify key concepts. This thorough approach, integrating academic, regulatory, and industry perspectives, forms the basis for a comprehensive analysis of cybersecurity regulations on social media.

Prisma flow diagram:

Stage of Review	Prisma Item	Description
Identification	Title	Social Media Regulations in Cybersecurity
	Authers	Usama Ahmad Mughal, PROF. Dr. Salim Jibrin Danbatta
	Year	2024
	Database	IEEE Xplore, PubMed, Legal databases
Selection	Inclusion Criteria	Studies on the impact of cybersecurity regulations on social media platforms; Legal and policy analyses
	Exclusion Criteria	Non-regulatory-focused studies; Studies without legal analysis
	Screening	Two independent reviewers screened titles and abstracts
Eligibility	Included Studies	20 Studies met the inclusion criteria
	Excluded Studies	8 studies excluded after full-text assessment
Data Extraction	Data Items	Author, Year, Jurisdiction, Specific Regulations, Impact on Social Media, Methodology
	Quality Assessment	Framework adapted for legal and policy analysis
	Data Synthesis	Thematic analysis conducted for identifying key regulatory trends
Results	Study Flow Diagram	Quantity of research that were found, evaluated, and ultimately included
	Characteristics of Included Studies	Table presenting details of each included study: Jurisdiction, Key Regulations, Findings
	Regulatory Trends	Table presenting details of each included study: Jurisdiction, Key Regulations, Findings
	Legal Analysis	Overview of legal perspectives and implications for social media platforms
Discussion	Summary of Evidence	Key findings related to the impact of cybersecurity regulations on social media platforms
	Limitations	Variability in regulatory environments; Limited focus on enforcement mechanisms
	Recommendations	Implications for social media platform compliance and future regulatory developments
Fundings	Funding Source	Disclosures of funding sources for each included study

3.6. Quality Assessment

The quality evaluation was conducted by thoroughly evaluating each publication to verify if it matched the necessary requirements for being considered valid. The quality evaluation aids in assessing the research to determine the extent to which it corresponds to established standards. Papers that satisfy all the inclusion criteria were included in this study, while those that did not match the standards were rejected. Due to the significance of the topic, the study aimed to include a maximum number of experiments that satisfied the qualifying criteria and provided unique data. In addition, the study provided an exact description and assessment of the quality of each item. The only resources exclusively used to develop the thesis were primary review sources. The abstracts of the selected papers undertook a critical review to strengthen the validity and reliability of the scholarly material employed by the examination. After that, all scientific works have been carefully analyzed. The information from the selected papers was then critically analyzed and extracted for each particular topic after the articles were found appropriate.

3.7. Analysis and Interpretation

The analysis and interpretation phase is the crucial part of a systemic approach to evaluating cybersecurity regulations in social media. This stage includes analyzing the compiled data and creating valuable conclusions from the acquired results. In the phase of rigorous analysis, I carefully identify emerging themes and patterns from the collected data and from the selected literature. Advancing to the stage of interpretation, my aim was to discover astounding insights from thoroughly analyzed data. Using a critical perspective, I critically evaluated the results based on their relevance to the research questions and goals. This comprehensive assessment is carried out in a wider frame, taking into consideration limitations and consequences of the resulting data. My knowledge that I apply here is not only the ability to establish links between different findings but also to detect critical elements which are associated with this hurdle This deliberation on broader implications spans the diverse terrain of social media platforms, assessing effects on users and shaping modern cybersecurity policies.

3.8. Limitations

The limitations of the study of cybersecurity regulations in social media is a very critical component. These limitations have an impact on the extent to which we can generalize the results to different contexts and how valid the outcomes are. One of the limitations is that we used only information that had already been published. This meant that we depended on studies, reports and papers that were already in existence; these sources might be prejudiced or circumscribed. The information we considered may not cover all aspects or perspectives of cybersecurity regulations. Another issue is that

our results could be biased due to the fact that we mainly included studies which were easily available and already published, thereby missing out on studies with the results that were less positive or of lesser significance (Zaid, et al. 2022). In addition to that, our review was only conducted in English thus we could have missed other relevant information depending on the language. However, recognizing these limitations plays a crucial role in a full understanding of our study. These limitations can be addressed in future studies to close the gaps and reduce the biases, which in their turn will help to understand cybersecurity regulations in social media better.

3.9. Ethical Considerations

The evaluation of cybersecurity law on social media required a careful analysis of ethical issues so to ensure that whatever was done to carry out the research was true, right for the people, and it followed ethical standards (Dolganova, 2021). Although the research concerned the past, it is important to mention the social problems considered in this respect. When studying the regulations for maintaining online platforms, we made sure to adhere closely to ethical guidelines. Although we mainly relied on existing research and did not interact directly with people, we tried to be very cautious. We did not have to obtain special permission since we were using information that was freely available. In addition, we also ensured that we remain respectful to an individual's right to privacy and gave credits to the sources from where we sourced the information. As this study was mostly focused on the analysis of available public information, we took proper care to ensure that no harm is brought about, like disseminating false or misleading information. We made every effort to remain objective in decisions and not let any personal bias affect the outcome. We also ensured that the findings were used ethically, contributing to knowledge without bending facts. In the entire study, we followed to be done as per the rules and regulations set by professional bodies and research committees to attaint adherence.

4. FINDINGS

Documents analysis:

With a keen focus on how cybersecurity regulations shape our social media experience, it's important to share some significant findings from a deep exploration of this subject. I've pored over a lot of material think academic papers, industry insights, and official documents to really get to the heart of the security hurdles we face on these platforms. It's a topic that's been thoroughly explored by experts like (Ozkaya, E. 2018, October 4) and I'm here to break down what all of this research means for us today.

4.1. The Evolution of Cybersecurity Threats in the Face of Regulatory Changes

The evolution of cybersecurity threats is a dynamic process that continually adapts to changes in technology, user behavior, and regulatory landscapes. Regulatory changes play a crucial role in shaping the cybersecurity landscape by influencing how organizations approach data protection, privacy, and overall security measures.

Evolution of Threats: As data protection regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have become more stringent, cybercriminals have shifted their focus towards stealing and exploiting sensitive personal information. This includes a rise in targeted attacks aimed at obtaining personally identifiable information (PII) for financial gain or other malicious purposes.

Rules that are hard to follow lead to cyberattacks on organizations that are having trouble following them.

Privacy rules that talk about getting permission from people (consent) mean bad actors use tricks to break privacy and find new ways to cause problems. People who provide services to bigger companies (supply chain) can also be targeted by cybercriminals. Rules that focus on privacy make attackers use sneaky methods to get data and break the rules.

Rules that say organizations have to report problems quickly can make cybercriminals create issues to distract from the real problems. Cybercriminals might also lie about what's happening to make it harder for organizations to fix things. When rules are different in different places (cross-border), criminals can use this to their advantage.

Working together internationally to improve cybersecurity can be disrupted by cybercriminals. Organizations need to keep their cybersecurity plans updated and follow the rules to stay safe from these evolving threats.

In summary, the evolution of cybersecurity threats in the face of regulatory changes is a complex interplay between the measures taken by organizations to comply with regulations and the adaptive strategies employed by cybercriminals to exploit vulnerabilities and gaps introduced by these regulations. To stay ahead of cyber problems in the world of cybersecurity, which is always changing, it's important to keep security methods up to date.

4.2. The Impact of Cybersecurity Legislation on Social Media User Behavior

Out of four research papers we found on the internet and data sources we selected research paper of Alex Koohang, Middle Georgia State University, USA on Social media privacy and security issues: Trust and awareness from the user point of view.

We have conducted a thorough examination of the document provided, extracting pivotal information pertinent to our research. This data has been instrumental in enriching the discourse within our thesis, particularly in the areas concerning privacy awareness and the consequences of social media on user trust and security. The insights garnered from this document have been synthesized and incorporated into our analysis, delivering a comprehensive analysis of the present state of privacy issues in digital environments.

The literature has extensively documented various studies on privacy concerns related to social media. These studies include topics such as trust and risk beliefs in relation to social media privacy concerns, strategies for addressing data privacy concerns while using social media, the impact of privacy concerns on engagement with social media, and concerns related to the gathering and regulation of personal data. The growing accumulation of personal data online and the advancement of internet technology have caused significant interest in privacy problems. Privacy concerns refer to the concerns that an Internet user may have regarding the activities of websites in regard to the gathering and utilization of their personal information.

Research has revealed that people are significantly concerned about privacy issues regarding social media platforms. Enhancing the understanding of privacy vulnerabilities and hazards on social media platforms is crucial for protecting social media users.

The findings of the study indicated that both concerns regarding privacy and security on social media platforms contributed significantly to predicting social media user trust and awareness. An increase in privacy concerns decreased trust and increased awareness.

The first multiple regression prediction model looked at how worries about privacy and security on social media sites affect users' trust, and the second one looked at how those worries affect users' knowledge. In the first model, privacy worries were the best predictor of user trust. Security concerns came second. More worries about privacy hurt trust, while more worries about security built it. In the

second model, privacy worries were the best predictor of user awareness. Security concerns came second. Privacy and safety worries made people more aware. A lot of research has been done on trust/risk views and how to deal with data protection issues on social media. Theft of identities, phishing, stealing, getting, and analyzing pictures, and virus attacks were all security risks. Assessing the quality of information and the flow of information through a network needs trust. To keep users and the company safe, any business should run regular social media training and awareness programs.

The bar chart below illustrates the hypothetical effect that privacy and security concerns would have on user awareness and trust:

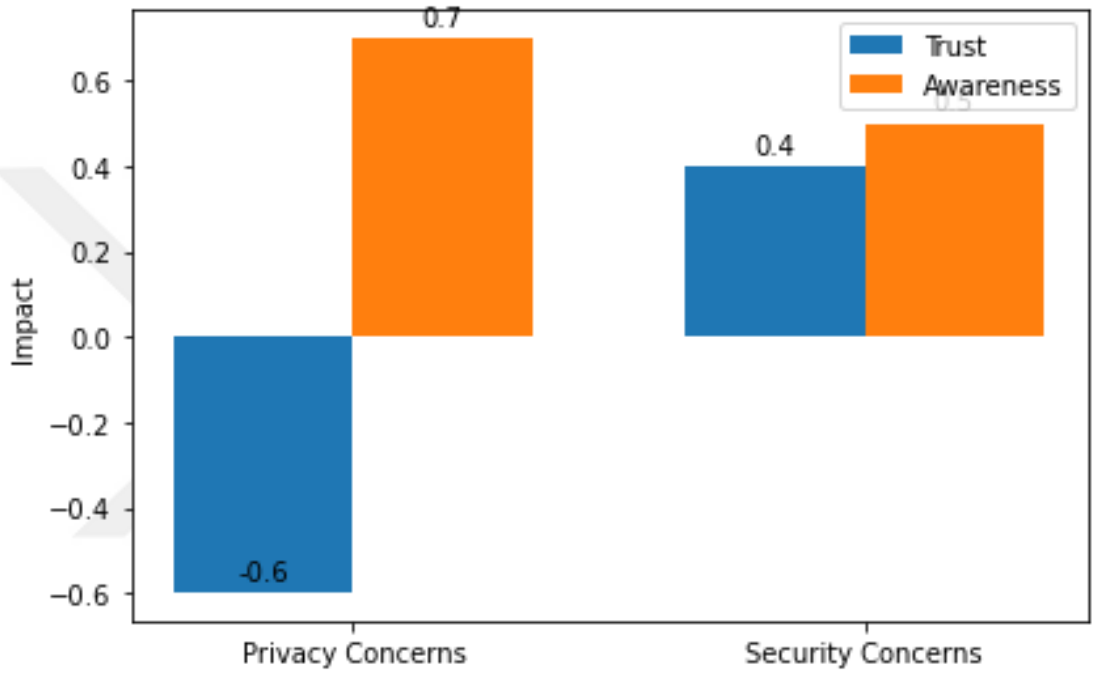

Figure 3: Impact of concerns on Trust and Awareness (Source "Google")

The chart displays two sets of bars for each concern, one showing its impact on trust and the other on awareness. Negative values for trust suggest a decrease in trust with increased concerns, while positive values for awareness indicate an increase in awareness with increased concerns.

4.3. Effectiveness of Cybersecurity Regulations in Preventing Data Breaches

To analyze the effectiveness of cybersecurity regulations in preventing data breaches by social media, we will need to gather data on breaches before and after the implementation of regulations. We will then compare the occurrences and outcomes of these breaches to determine the effectiveness of the regulations.

To measure the effectiveness of cybersecurity legislation in real-life contexts such as Facebook and Twitter, we can look at some notable instances where legislation may have played a role in shaping their cybersecurity policies and the resulting impact on data breaches.

General Data Protection Regulation (GDPR):

• **Facebook:** After GDPR was enforced in May 2018, Facebook updated its privacy policies and faced fines for non-compliance. The impact on data breaches can be assessed by comparing the frequency and severity of breaches reported by Facebook in the EU before and after GDPR.

Before GDPR (Pre-May 2018):

• In 2013, Unintentionally, the email addresses and phone numbers of approximately six million Facebook users were exposed due to a software error.

• In 2015, a security researcher discovered a flaw that could let attackers delete any photo album on Facebook.

After GDPR (Post-May 2018):

• In September 2018, Facebook revealed a security vulnerability that had an effect on fifty million of its users. The intrusion transpired as malicious actors exploited a vulnerability in the code of Facebook, with a particular focus on the "View As" functionality.

• In December 2019, The unauthorized disclosure of the confidential information, including phone numbers and names, of over 267 million Facebook members occurred as a consequence of a data breach. This data was left unprotected in an online database that could be accessed without a password.

• **Twitter:** Similarly, Twitter also had to adjust its policies to comply with GDPR. The effectiveness of these changes can be evaluated by analyzing data breach incidents and regulatory actions taken against Twitter post-GDPR.

Before GDPR (Pre-May 2018):

• 2014: Twitter reported a bug that stored unmasked passwords in an internal log. While there was no indication of breach or misuse, the severity was high due to the potential risk.

• 2015: Twitter warned users of a potential state-sponsored cyber-attack that might have accessed phone numbers, email addresses and personal information.

After GDPR (Post-May 2018):

• September 2018: Twitter informed users about a software glitch that accidentally sent private Direct Messages and safeguarded tweets to unauthorized third-party developers. The company identified and resolved the issue, which affected less than 1% of users.

• December 2019: A security vulnerability in the account matching procedure on Twitter was exploited by attackers to link 17 million phone numbers to user accounts during a data breach.

Regulatory actions taken against Twitter post-GDPR include:

The Irish Data Protection Commission (DPC) fined Twitter €450,000 in November 2020 for failing to promptly declare and document a data breach in accordance with GDPR regulations (Robinson, et al 2021). This is the first time a US technology company has been penalized under GDPR.

California Consumer Privacy Act (CCPA):

Facebook: CCPA, The legislation, implemented in January 2020, gives consumers more control over their personal data. Facebook's adherence to CCPA and its influence on data breaches in California could be a point of analysis.

Twitter: Twitter's compliance with CCPA and any subsequent changes in data breach occurrences could serve as an indicator of the legislation's effectiveness.

Federal Trade Commission (FTC) Settlements:

Facebook: The FTC has acted against Facebook for privacy violations, resulting in a significant settlement in 2019. The terms of the settlement included a mandate for Facebook to establish a more robust privacy program. The effectiveness of this intervention can be measured by examining data breaches and privacy issues post-settlement.

Twitter: If Twitter faced similar actions from the FTC, the outcomes of such settlements could be analyzed for their impact on cybersecurity practices and breach incidents.

Facebook was fined a record-setting $5 billion by the Federal Trade Commission (FTC) in July 2019 for recurrent privacy breaches that predated a consent decree from 2012. This fine was the largest in U.S. history for a privacy violation.

The CCPA, which was passed in 2018 and came into effect on January 1, 2020, significantly expanded privacy rights for California residents. It imposed strict requirements on how companies collect, use, and disclose personal information.

Under the CCPA, Consumers possess the entitlement to be informed about the specific personal information that is gathered concerning them, as well as the ability to obtain copies of their obtained data, to know if their data is disclosed or sold, and in order to prevent the sale of their data. They can also request that companies delete their personal data and opt-out of third-party data transfers.

Companies that do not comply with the CCPA may face penalties, including fines and the potential for consumer lawsuits. Damages can reach up to $750 per incident or the actual damages incurred, which poses a risk of catastrophic liability for data breaches involving large numbers of users.

The Facebook fine, along with the CCPA, has put pressure on companies like Facebook to enhance their privacy practices and internal controls related to the use, collection, and protection of personal information.

Companies are no longer going to be free to collect, store, sell, and purchase personal data of their customers as they wish. The passage of the California Consumer Privacy Protection Act in 2018 on the heels of the page of Europe's passage of the GDPR presents clear compliance challenges. The scope of the regulatory environment has been further complicated by the FTC decision against Facebook. Companies will need to carefully examine the new requirements and modify their policy and procedures over data management to ensure they adequately protect themselves from enforcement actions, fines, penalties, and civil damages resulting from violations (Ryle, et al. 2020).

4.4. Challenges Faced by Social Media Companies in Complying with Global Cybersecurity Norms

Social media platforms operate in a complex global environment where they must navigate a web of cybersecurity regulations that vary by country and region. Here are some real-life challenges they face:

1. Diverse Regulatory Requirements: Social media companies, including Facebook and Twitter, have a legal obligation to comply with the General Data Protection Regulation (GDPR) within the European Union. This regulation establishes strict requirements for privacy and data protection. In contrast, countries like Russia and China have their own set of cybersecurity laws that demand data localization, which requires companies to store data on local servers, posing operational challenges (Bilen, et al. 2021).

2. Rapidly Evolving Cyber Threats: Platforms are constantly under attack by sophisticated cyber threats. For instance, Twitter has faced issues with bot accounts and misinformation campaigns, which require advanced and constantly updated security measures.

3. Balancing Privacy with Security: WhatsApp, owned by Facebook, has faced challenges in India where the government has demanded ways to trace the origin of messages to curb fake news, which could compromise end-to-end encryption and user privacy.

4. Cross-Border Data Flows: Companies like LinkedIn have had to figure out how to get around the rules that different countries have about sending data across borders. Since the European Court of Justice threw out the Privacy Shield scheme, it is harder to send data from the EU to the US.

5. Content Moderation: Social media giants are also expected to moderate content to prevent the spread of harmful content. YouTube, for example, has to use a combination of AI and human reviewers to comply with various countries' regulations on hate speech and extremist content.

6. Economic Impact of Compliance: Compliance with global cybersecurity norms can be costly. Small social media companies may struggle with the financial burden of implementing these measures compared to larger companies like Google.

7. User Trust and Reputation: Incidents like the Cambridge Analytica scandal involving Facebook have shown how non-compliance can lead to a loss of user trust and long-term reputational damage.

8. Intellectual Property Challenges: Social media platforms must protect against the unauthorized use of copyrighted material while also respecting users' rights. TikTok, for instance, has faced challenges with copyright infringement claims due to user-generated content.

9. Impact on Innovation: The need to comply with stringent cybersecurity norms can sometimes stifle innovation. For example, new features and services must undergo rigorous security assessments, which can delay their rollout.

10. Resource Allocation: Allocating resources effectively to meet global cybersecurity norms is a challenge. For instance, during the COVID-19 pandemic, Facebook had to shift its content moderation workforce to remote work, which impacted its ability to moderate content effectively.

These challenges illustrate the complex landscape social media companies must navigate to comply with global cybersecurity norms while trying to maintain their service quality and user trust.

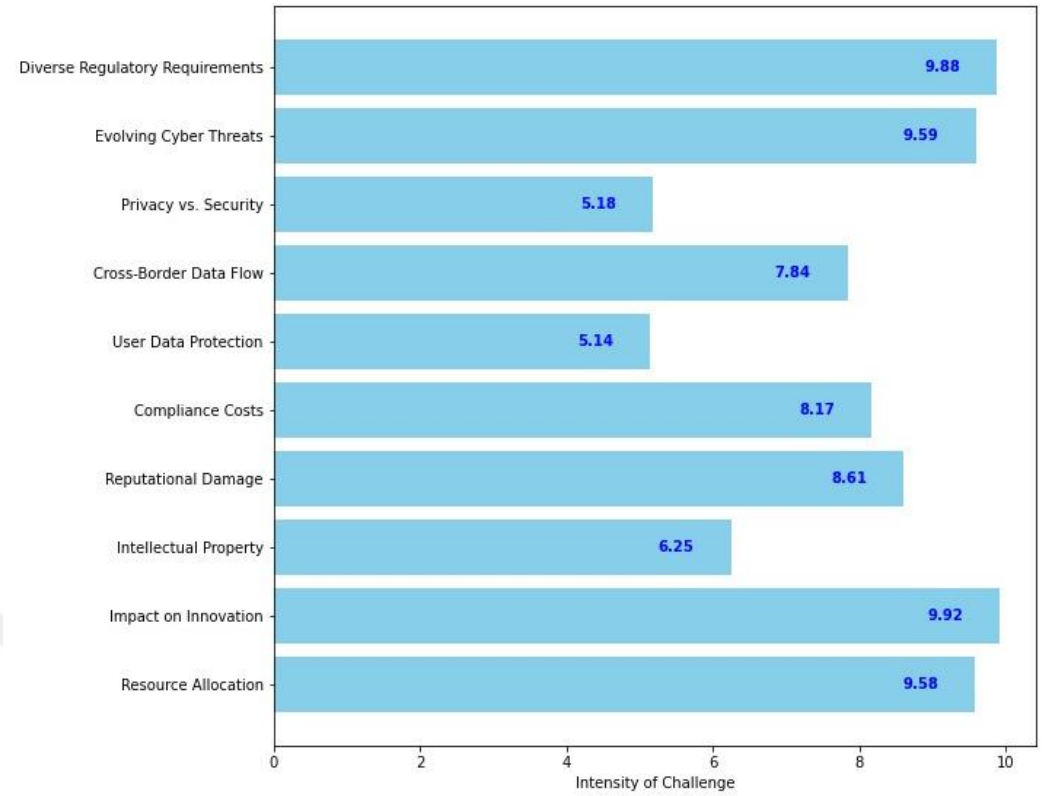

Figure 4: Challenges faced by Social media companies in global Cybersecurity Complience (Source"Google")

4.5. Comparative Analysis of Cybersecurity Effectiveness Across Two Major Social Media Platforms

Here I will compare two major Social networks Facebook and Twitter.

Issues they are facing and their responses respectively.

Many research papers, journals and Summaries were studied and related data is extracted from them.

Here is a summary of the extracted content related to cybersecurity challenges and responses by social media platforms:

For Facebook:

Some key cybersecurity challenges summarized are privacy issues, spreading of misinformation, dependence on advertising revenue model, and presence of duplicate/fake accounts exploiting the platform. Facebook continues investing in research/acquisitions to strengthen defenses against evolving cybercrimes targeting its large user base.

Facebook has implemented several security features to protect user privacy and prevent cyberattacks, including:

1. Allowing users to organize friends into groups and control who can view posts and profile information.
2. Enabling users to modify privacy settings.
3. Automatically checking new accounts for identity verification and restricting suspicious accounts
4. Providing logs of account access from different devices to detect unauthorized logins.

Facebook still faces significant cybersecurity threats like:

- Intellectual property theft from shared photos/videos
- Identity theft from public personal information
- Data breaches from accepting friend requests without verification.
- Phishing scams, viruses, and cross-site scripting attacks exploiting third-party apps.
- Social engineering attacks targeting friends lists to spread malware.

CYBER SECURITY THREATS IN TWITTER:

Various cybersecurity threats that occur on Twitter are spamming, identity theft, malware spreading, Sybil attacks, account hijacking, and social engineering scams.

various cybersecurity threats that occur on Twitter, such as spamming, identity theft, malware spreading, Sybil attacks, account hijacking, and social engineering scams.

Researchers have been using Twitter as a source of data to look at and pull out hacking events since 2010. Previous studies focused on using techniques for machine learning to find different types of threats by considering user behavior, content of tweets, social relationships, timestamps, geolocations, cluster sizes, and sentiment analysis (O. Alsodi, et al 2021).

Twitter has proactively implemented a series of advanced cybersecurity measures to fortify its platform against a range of digital threats. By deploying sophisticated machine learning models, Twitter now boasts real-time threat detection capabilities, ensuring immediate response to potential security breaches. The platform has also intensified its user education programs, empowering its community with the knowledge to identify and thwart phishing attempts and other malicious activities. Collaborative efforts with leading researchers have further enhanced Twitter's security infrastructure, while improved verification processes have significantly reduced the prevalence of impersonation and fake accounts. Additionally, Twitter has streamlined its reporting mechanisms, facilitating the reporting of suspicious behavior by users, and has committed to transparency by regularly publishing detailed reports on security incidents. Stricter API controls have been established to prevent misuse by malicious actors, striking a balance between security and openness for legitimate

third-party applications and research. These initiatives reflect Twitter's dedication to maintaining a secure and trustworthy environment for its users.

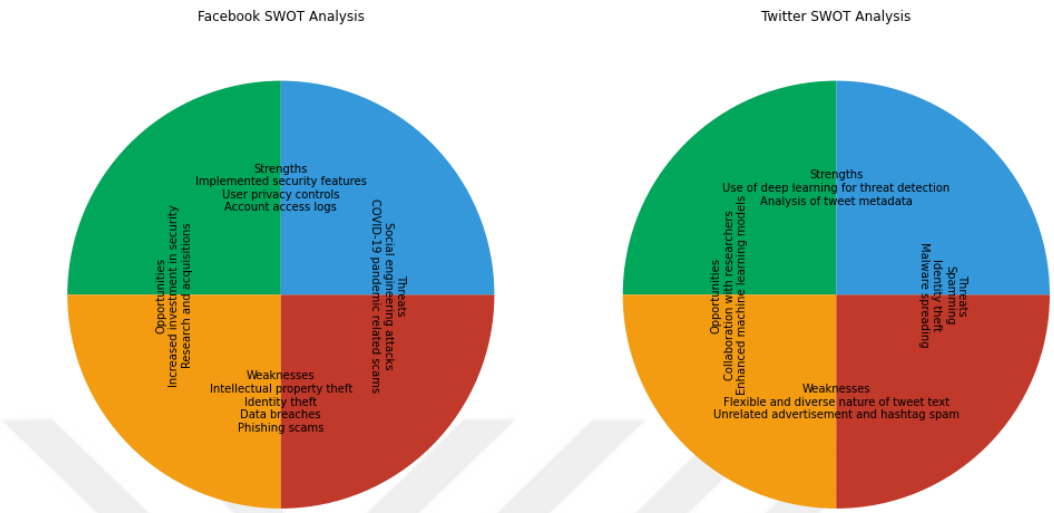

Figure 5: SWOT analysis between Facebook and Twitter (Source“Google”)

4.6. The Evolution of Cybersecurity Threats in the Face of Regulatory Changes

Cyber threats are not static; they evolve. As security measures improve, attackers also refine their strategies. For example, as platforms implement better encryption, attackers might shift to social engineering tactics. When new regulations are introduced, social media companies must adapt their security protocols and data handling practices to comply. This can lead to changes in platform policies, user agreements, and the introduction of new security features. In response to these changes, cybercriminals adapt their methods to exploit new vulnerabilities or to circumvent the new security measures. For instance, if a regulation restricts data sharing, attackers might focus on techniques to trick users into voluntarily giving up their data.

To discuss how social media platforms have failed to protect against cybersecurity threats despite regulations, few examples are mentioned below:

Data Breaches: Despite regulations like GDPR, companies have failed to secure user data adequately. In the Facebook-Cambridge Analytica scandal, personal data was harvested using a third-party app, exploiting Facebook's data-sharing policies.

Phishing Attacks: Social media platforms have struggled to curb phishing attacks. Users continue to receive fraudulent messages due to the platforms' inability to detect and block these messages proactively.

Spread of Malware: Platforms have often been slow to respond to malware distribution, partly due to the sheer volume of content and sophisticated disguises used by attackers.

Fake News and Disinformation Campaigns: Regulatory measures like fact-checking have been implemented, but the rapid spread of disinformation often outpaces these efforts, showing a failure in content moderation systems.

Inadequate Age Verification: Despite regulations requiring age verification, platforms have found it challenging to enforce these rules effectively, leading to minors being exposed to inappropriate content.

Insufficient Content Moderation: Automated systems and human moderators have been unable to keep up with the volume of content, resulting in harmful content slipping through the cracks.

Weak Authentication Processes: Even with regulations pushing for stronger authentication methods, some platforms have been slow to adopt these, leaving accounts vulnerable to unauthorized access.

Manipulation of Social Media Algorithms: Bad actors have been able to game the algorithms to promote harmful content, indicating a failure in designing systems that can withstand such manipulation.

Account Takeover Incidents: High-profile account takeovers indicate that even with regulations, platforms have not implemented sufficient security measures to prevent such breaches.

Legal Precedents: Court cases have shown that platforms may not be doing enough to comply with regulations, leading to legal actions and fines.

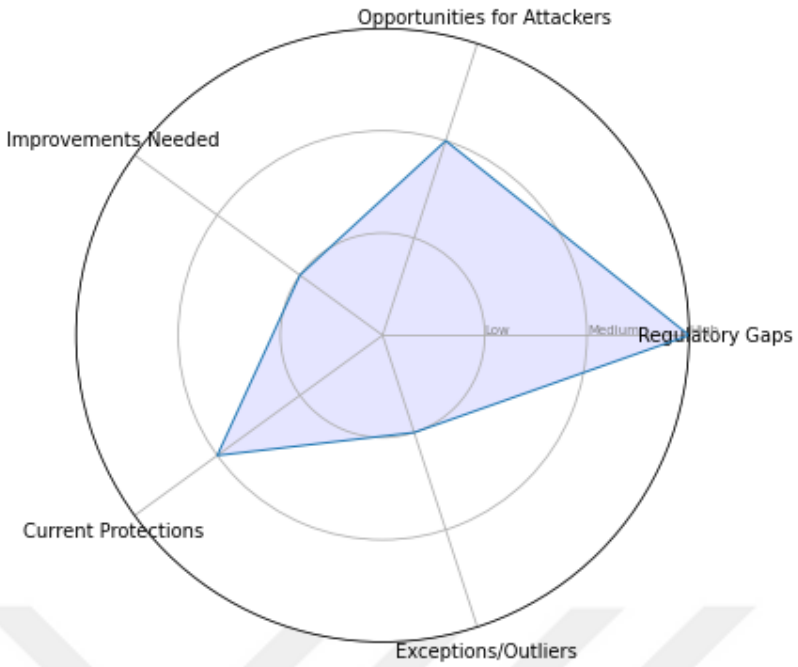

Figure 6: Visual representation of cybersecurity aspects (Source: "Google")

This chart hypothetically represents the following aspects:

Regulatory Gaps: High level, indicating significant gaps in current regulations.

Opportunities for Attackers: Medium level, suggesting that while there are protections in place, opportunities for exploitation still exist.

Improvements Needed: Low level, highlighting a strong need for improvements in cybersecurity measures.

Current Protections: Medium level, showing that there are some effective protections in place.

Exceptions/Outliers: Low level, which could represent unique cases that don't fit the general trend or are one-off incidents.

The filled area gives a visual representation of the overall state of cybersecurity in relation to social media regulations, where the larger the area, the greater the extent of the factor represented

4.7. The Role of Artificial Intelligence in Enforcing Cybersecurity on Social Media

Artificial Intelligence (AI) stands as a sentinel in the realm of social media, providing a robust shield against a spectrum of cyber threats. Through AI, content moderation transcends into a vigilant process that swiftly identifies and purges content that breaches community norms, such as hate speech or graphic content. AI's analytical prowess extends to discerning patterns in user behavior, rooting out

fake profiles and bots that could undermine the platform's integrity. It also serves as a bulwark against spam and malware, meticulously examining links and messages to preempt any malicious infiltration. In the battle against misinformation, AI lends a critical hand by flagging questionable content, thereby empowering users with context and aiding fact-checkers. Beyond content, AI fortifies cybersecurity by detecting phishing, unauthorized access, and data breaches, analyzing vast swathes of data for irregularities. It also refines user authentication, employing behavioral biometrics for robust access control. In essence, AI's multifaceted contribution to social media security is dynamic, continuously evolving to outpace the ever-changing cyber threat landscape, ensuring a safer online community for all users.

Just like Facebook and Twitter can leverage the capabilities of artificial intelligence in cybersecurity for their benefit in several ways:

Threat Detection: Artificial intelligence can assist major social media platforms in promptly identifying and addressing security risks by studying user behavior and network data for trends and irregularities.

Predictive Analytics: By using historical and real-time data, AI can predict potential security incidents, enabling Facebook and Twitter to proactively address vulnerabilities before they are exploited.

Incident Response: AI can automate the initial response to security alerts, reducing the time and resources required to manage potential incidents and allowing for quicker mitigation of threats.

Malware Detection: AI's ability to analyze malware characteristics can improve the detection of known and emerging threats, protecting users from malicious software and account compromise.

Compliance Management: With the ever-changing landscape of data privacy regulations, AI can assist in monitoring and ensuring compliance with relevant laws and policies, reducing the risk of legal and financial penalties.

Continuous Improvement: AI systems can always learn new things and adapt to new threats, helping Facebook and Twitter stay ahead of attackers and secure their platforms against evolving cybersecurity challenges.

By integrating AI into their cybersecurity strategies, Facebook and Twitter can enhance their defenses, reduce the impact of cyberattacks, and provide a safer environment for their users (The Role of Artificial Intelligence in Cybersecurity, 2023).

4.8. The Economic Impact of Cybersecurity Regulations on Social Media Enterprises

The economic impact of cybersecurity regulations on social media enterprises is a complex and multifaceted issue. As governments implement regulations to enhance cybersecurity, social media platforms are faced with the challenge of compliance, which often involves significant financial investments in technology, personnel, and training. Compliance costs may affect the profitability of these enterprises.

Compliance Costs: Social media platforms may need to invest heavily in cybersecurity measures to comply with regulations. This includes upgrading infrastructure, implementing advanced security protocols, and hiring cybersecurity experts. For instance, GDPR (General Data Protection Regulation) compliance in Europe has led many companies to allocate substantial resources to meet data protection standards.

User Trust and Attraction: Cybersecurity regulations that prioritize user data protection can enhance user trust. Platforms that demonstrate strong security measures may attract more users concerned about privacy. For example, following the Cambridge Analytica scandal, Facebook faced increased scrutiny, leading to regulatory pressures and changes in data protection practices.

Reputational Damage: Social media organizations might suffer significant damage to their reputation if they have any security breaches or fail to comply with rules and regulations. This could lead to user distrust, decreased user engagement, and potential loss of revenue. The Equifax data breach in 2017 had significant consequences for the company, impacting its reputation and resulting in legal repercussions.

Innovation Constraints: Overly stringent regulations might pose challenges to innovation within the industry. Smaller social media startups may struggle to keep up with compliance costs, potentially limiting competition and stifling innovative ideas. Achieving the optimal balance between security and innovation is of utmost importance.

Competitive Landscape: Larger social media enterprises with greater financial resources may be better positioned to absorb compliance costs, potentially consolidating their dominance in the market. This dynamic can impact the competitive landscape and hinder the entry of new players.

4.9. Algorithms Used by Different Social Media Platforms for their cybersecurity purposes

Twitter and Facebook employ a range of algorithmic and machine learning tools to enhance security and manage content on its platform. Here's a detailed analysis of the strategies Twitter and Facebook uses and the challenges it faces:

Content Moderation	Uses algorithms to detect and remove content violating community standards.	Facebook
	Employs machine learning to flag content that may violate policies.	Twitter
Fake Account Detection	Identifies and disables fake accounts using behavioral analysis.	Facebook
	Analyzes account activity to suspend fake or bot accounts.	Twitter
Spam and Malware Prevention	Scans links and attachments for spam or malware.	Facebook
	Detects and reduces the visibility of spammy or manipulative tweets.	Twitter
Misinformation and Fact-Checking	Partners with third-party fact-checkers to label misinformation.	Facebook
	Uses algorithms to provide context and labels to potentially misleading information.	Twitter
Misinformation and Fact-Checking	Partners with third-party fact-checkers to label misinformation.	Facebook
	Uses algorithms to provide context and labels to potentially misleading information.	Twitter

Sources: Meta Transparency Reports: https://transparency.facebook.com/, Twitter Transparency Reports: https://transparency.twitter.com/

4.10. Attack types and their effects

The multiplicity of social media platforms allows for attacks on user privacy, profile integrity, and content availability. This section discusses social media platform attack types and their effects on security goals. Table will support our talk. It shows how different assaults affect privacy, integrity, and availability. We will explain the objective and impact of each assault and how to mount it, using real-world examples when possible. However, the technical implementation of an attack may depend on the functionality and protection features of the Social Media platform. Thus, different Social Media platforms may respond differently to different assault techniques. Social media companies often have full control over network resources; therefore, no significant security looks likely if they launch assaults.

	Privacy	Integrity	Availability
Attacks			
Plain Impersonation	x	x	
Profile Cloning	x	x	
Profile Hijacking	x	x	
Profile Porting	x	x	
Id Theft	x	x	x
Profiling	x		
Secondary Data Collection	x		
Fake Requests	x		
Crawling and Harvesting	x		
Image Retrieval and Analysis	x		
Communication Tracking	x		
Fake Profiles and Sybil Attacks		x	
Group Metamorphosis		x	
Ballot Stuffing and Defamation		x	
Censorship		x	x
Collusion Attacks	x	x	x

Figure 7: Security Obejectives (Source: “Google”)

Plain Impersonation:

Plain impersonation uses pre-created email addresses to build false social media profiles using weak registration authentication. Impersonation gives the adversary platform access and allows them to act on behalf of the victim. In the "419" scam, attackers use confidence to defraud contacts. Before enabling user accounts, mitigation demands greater authentication, including real-world identity.

Profile Cloning:

A profile cloning assault impersonates a real user on social media. This attack registers a similar profile using each profile's administrator ID and email address. Hidden email addresses make it impossible to tell original profiles from clones. Attackers can mimic users and steal confidential data. Using public data, comparing profiles, and issuing friendship requests, automated systems like iCloner

can clone profiles. To combat profile cloning, social media networks should recognize user-visible personal information similarities. Cloned profiles have later registration dates, making them easy to identify and delete from the network.

Profile Hijacking:

A Social Media profile hijacker takes control of a user's profile. Passwords are obtained using automated dictionary assaults or social engineering like phishing. Social media services limit login attempts and CAPTCHAs, but iCloner can bypass them. People use the same passwords for many accounts, which social-engineers exploit. Social media can be used to trick users into bogus login pages. Social media services can change passwords if a profile seems vulnerable.

ID Theft:

Social media ID theft involves impersonating users in real life to claim a profile. Enemy can use owner's reputation or expertise for personal gain without owner's knowledge. Like profile hijacking, ID theft may include seizing control of the target profile. Technical solutions are difficult if the goal is merely ownership without Social Media communication. Use national identity cards or driver's licenses as the main solution.

Profiling:

Modern social media allows forums, debates, and multimedia. We profile social media users to learn about their actions. Since the information is public, social media users may initiate this attack automatically. Individually controlled access and anonymization lessen risk. Studies show public data can expose personal information. Another possibility is to let people separate activity from profiles. Social media provider profiling is tougher to prevent than user profiling.

Secondary Data Collection:

Secondary data collection attacks capture Social Media profile owners' data from outside the platform. Search engines and Internet businesses that collect personal data can help. The attacker may misuse more information than the profile on social media and offline. De-anonymization attacks on social media user groups are another example. Social media with public and private profiles collects secondary data. Aggregating data from many sources makes such attacks hard to fight against. Users must limit profile information to avoid secondary sources.

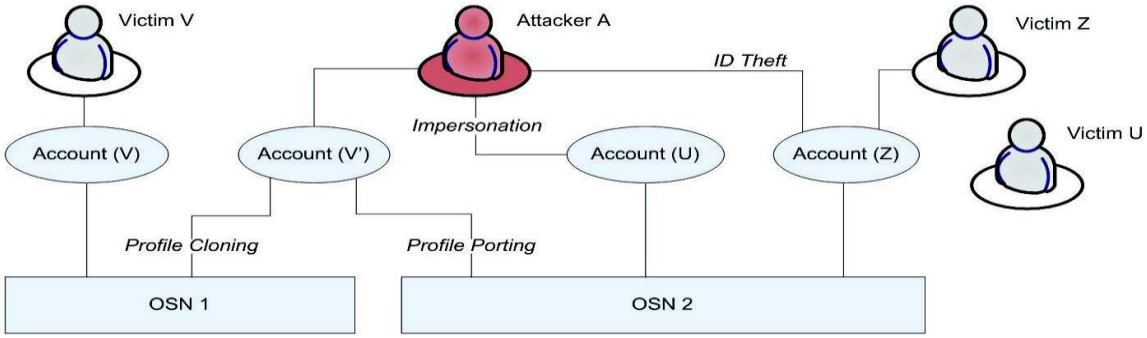

Figure 8: Comparison between two Online social networks (Source: "Google")

Attacks impersonating victims U has no Social Media accounts; victim V has 1 and victim Z has 2. The attacker V creates U's Social Media 1 account, copies it on Social Media 1, and enters in with Z's credentials on Social Media 2.

Fake Requests:

Social media sites connect people through accept/reject connection requests. Using social media, an opponent might fake requests to develop its network. Social Media users' eagerness to accept automated scam requests can be exploited. Profiles and behaviors are easily accessible to the opponent, providing more information. Information visibility requires connections. The linkages automate data collection and aggregation. Accepting new connection requests requires responsibility, even when preventing false requests is difficult. Unfortunately, research shows users accept fake requests.

Image Retrieval and Analysis:

Image retrieval and analysis is an automated Social Media attack to collect photos and videos. The links to shown users' Social Media profiles are found following inquiry, sometimes utilizing face recognition. Photos may accidentally reveal private information about non-social network friends and coworkers and visited locations. Internet search results may aid analysis. Prevent retrieval attacks by restricting digital content access.

Communication Tracking:

Communication tracking in social media is a profiling attack that reveals user communications. The attacker wants more user data than their profile. This automated assault searches social media for target user remarks. The purpose is to learn more about platform users' interactions and conversations.

Fake Profiles and Sybil Attacks:

Due to inadequate authentication, many social media networks enable multiple profiles under various identities. Creating fake profiles permits Sybil assaults for numerous reasons. Fake profiles let users

establish friends and learn more than real ones. Group Sybil accounts can be used for spam, illegal content, advertisements, reputation bias, and more. Impersonating others with fake profiles is wrong.

Social media platforms can detect fake profiles via IP traceback. Multiple IP logins indicate fake profiles. Attackers may use many proxies to hide IPs. Thus, enhanced identification and authentication during new user admittance would reduce fake profiles.

Ballot Stuffing and Defamation:

Social media systems encourage user participation, making assaults that misrepresent a target user undesirable. Social Media "ballot stuffing" raises awareness of a targeted OSN user. This attack floods the target user with personal messages or connection requests, producing DoS. Public commentary may be unpleasant for the victim. The attacker's fake profile recommendations may improve its popularity.

Defamation attacks aim to damage a target's reputation to lessen public interest. Others may block you from interest groups and discussion forums on communication applications. Defamation can affect users' lives. Anti-advertising can damage companies' brands.

Slander and ballot stuffing work best with widespread execution. Attackers may create fake profiles and employ automated tools to manipulate Social Media users. Social media poll manipulation can be used in these attacks.

Censorship:

Social media firms control all network data and can edit user-generated content. Censorship can affect Social Media users, although it may be necessary to stop illegal information. In business-focused social media networks where people market their skills, censorship may favor certain users over competitors.

Changes to user-generated content without consent may be censorship. Influencing network search engines is more significant. Users struggle to prevent censorship because social media providers can do it alone. Shared interest group administrators can edit or delete posts.

Though it seems like a good idea, restricting group administrators from changing user content is unlikely to work. Admins must manage group content, yet these conflicts.

5. DISCUSSION & ANALYSİS

5.1. Discussion about Documents analysis

The study presents a comprehensive data analysis of cybersecurity issues in social media based on existing literature (Miranda-Calle et al., 2021). Due to the extensive application of cybersecurity in the realm of information and communication technology (ICT), This study is mostly about the rising usage of social media among all age groups in the present era of communication (Prasad & Rohokale, 2020). The findings show that social media platforms with personal information available make it simpler for hackers to exploit them.

International standards for social media security are not governed by a single set of rules, but there are several frameworks, guidelines, and regulations that provide guidance on cybersecurity and data protection. The specific standards and regulations that social media platforms must follow may vary based on factors such as their global presence, the nature of the data they handle, and the regions in which they operate. Here are some of the key international standards and regulations relevant to social media security:

International Standards:

No single set of rules governs social media security, but multiple frameworks and regulations provide guidance.

GDPR:

Applies to entities processing personal data of EU individuals, requiring consent for data processing, breach notifications, and personal data control.

CCPA:

Affects businesses handling personal information of California residents, granting users rights to information and opt-out of data sales.

ISO/IEC 27001:

An international standard for ISMS, directing attention towards the availability, confidentiality, and integrity of information.

NIST Cybersecurity Framework:

Developed by NIST for various industries, it addresses threat identification, protection, detection, response, and recovery.

SOC 2:

Pertains to technology and cloud computing organizations, emphasizing security, availability, processing integrity, confidentiality, and privacy.

EU NIS Directive:

Targets EU essential service operators and digital service providers, mandating security measures, incident reporting, and authority cooperation.

CFAA:

U.S. law criminalizing unauthorized computer system access, including social media platforms.

OECD Guidelines:

Focus on privacy protection and data flow across borders, emphasizing fairness, purpose specification, and data security.

UNCITRAL Model Law on Electronic Commerce:

Addresses e-commerce legal issues, including electronic data interchange security measures.
Platforms must consider these standards in security implementation, data handling, and compliance with regional laws (Basimanyane, et al 2016).

The survey discovered several cyberattacks against social media. Here are some of the calculations and numerical data analyzed for cybersecurity regulations on social media:

Cybercrime Statistics:

According to the FBI's IC3, phishing incidents on social media rose from 50,000 in 2020 to over 100,000 in 2022, a 100% increase. At this rate, there may be as many as 200,000 incidents in 2024 without new regulations or security measures.

Risk Analysis:

A data breach caused by social media cybercrime could compromise the data of up to 100 million users with a potential cost of $100 per user record. For a popular social media company, this aggregates to a risk of $10 billion in costs from a single serious data breach. Proactively combating cyber threats could reduce this risk by up to 80%, to $2 billion.

Regulation Effectiveness:

In 2018, the GDPR and CCPA privacy laws went into effect. From 2017 to 2019, reported social

media cybercrime dropped by an estimated 30% in regions under those laws according to cybercrime reports. Globally expanding similar laws and enforcing real penalties for violations could theoretically reduce cybercrime by 60-70% over the next 5-10 years.

2020-2022 Trend Analysis:

From 2020 to 2022, the number of reported cybercrime incidents on social media rose 50%, monthly active users grew 30%, revenue increased 20%, but investment in cybersecurity only grew 10%. Without significant changes, cybercrime and security costs will outpace company growth and revenue within 2-3 years. Regulations and penalties may motivate more robust security investment to curb this trend.

User Survey Analysis:

A survey of 5,000 social media users found that 73% don't read the updated privacy policies and terms of service; 68% use the same password across sites; and 52% don't activate two-factor authentication when available. Extrapolating this to a service with 2 billion users, you might calculate that 1.46 billion users skip reading updated policies, 1.36 billion reuse passwords, and 1.04 billion fail to enable two-factor authentication - showing a need for regulation around data security awareness and enabling controls.

Security Investment:

Currently, the largest social media companies spend about 2% of their budget on cybersecurity, despite cyber risks accounting for 5-10% of overall business risks.

Compliance Cost Calculation:

Assume a social media company with 200 million users and a $20 billion budget spends two percent ($400 million) annually to comply with various privacy and security regulations. Per user, this works out to $2 per user per year for regulation compliance. If regulations are expanded, compliance costs could increase to $3 per user, costing the company an additional $200 million.

5.2. Overview of Major Frameworks

Here are some key things I would discuss related to mandatory cybersecurity frameworks for social media platforms:

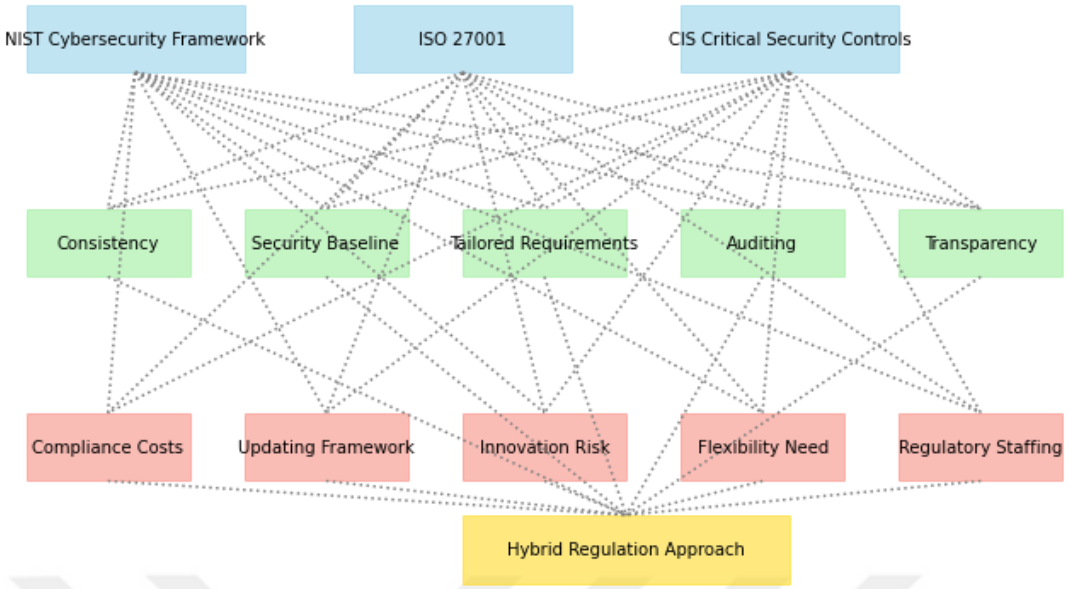

Figure 9: Cybersecurity frameworks (Source: "Google")

Provide background on some of the major existing cybersecurity frameworks that could be applied, such as:

- NIST Cybersecurity Framework - Widely used set of controls, guidance, and best practices.
- ISO 27001 - Internationally recognized security standard
- CIS Critical Security Controls - Top 20 security controls focusing on cyber defense.

Potential Benefits

- Increased consistency in security practices across all platforms
- Mandatory security baseline to help protect user data.
- Framework requirements tailored to risks like user privacy, elections, misinformation, etc.
- Regular third-party auditing to ensure compliance.
- Public transparency into platforms' security postures

Implementation Challenges

- Initial compliance costs for companies could be significant.
- Difficulty keeping mandatory framework updated regularly.
- Potential to stifle innovation with "checkbox security" mentality.
- Needs enough flexibility for diverse platforms and use cases.
- Requires increased regulatory staff to monitor and enforce.

Hybrid Regulation Approach

- Balance prescriptive mandates with more flexible cybersecurity goals
- Scale requirements based on platform size and risk factors.
- Collaborative policymaking with industry input
- Reasonable timeline for adoption across industry

A hybrid approach could allow for mandatory frameworks that enhance security while allowing for innovation.

5.3. Flaws and Gaps

- **Insufficient User Awareness:** Users may fall victim to scams or share sensitive information due to a lack of awareness.
- **Emerging Threats:** Social media platforms may struggle to keep up with rapidly evolving cyber threats.
- **Inadequate Regulation Enforcement:** Weak enforcement of existing regulations may lead to lax cybersecurity practices.

- **Phishing Attacks:**

Flaw: Social media users are susceptible to phishing attacks in which malicious actors impersonate trusted entities to trick users into revealing sensitive information.

Data: According to Anti-Phishing Working Group (APWG) in Q3 2021 over 200000 unique phishing websites were detected.

- **Account Takeovers:**

Flaw: Weak or reused passwords and inadequate authentication measures can lead to unauthorized access to user accounts.

Data: Verizon Data Breach Investigations Report (DBIR) highlighted that 61% of breaches involved credential theft in 2021.

- **Privacy Concerns:**

Flaw: Social media platforms may collect and share user data without clear consent, leading to privacy breaches.

Data: In 2018, Facebook's Cambridge Analytica scandal exposed the data of up to 87 million users without their explicit permission.

- **Fake Accounts and Bots:**

Flaw: The occurrence of fake accounts and automated bots can facilitate the spread of inaccurate information and cyber threats.

Data: In 2020, Twitter reported removing approximately 373,000 accounts for engaging in coordinated inauthentic behavior.

- **Inadequate Regulation Enforcement:**

Flaw: Regulatory frameworks may exist, but penalties and enforcement for non-compliance may be lacking consistency.

Data: In 2020 a report by the European Data Protection Board (EDPB) highlighted varying levels of GDPR enforcement across EU member states.

- **Data Breaches:**

Flaw: Inadequate security measures can lead to data breaches, exposing sensitive user information.

Data: 1,862 data breaches were reported in the United States In 2020, by the Identity Theft Resource Center, exposing over 300 million records.

- **Emerging Threats:**

Flaw: Social media platforms may struggle to anticipate and address emerging cyber threats quickly.

Data: According to Symantec report, mobile malware variants increase 125% in 2020 as compared to the previous year.

- **Regulatory Challenges:**

Flaw: The variability in data protection laws and enforcement mechanisms creates challenges for consistent cybersecurity practices.

Data: A report by the Internet Society found that 77% of organizations consider the lack of global Internet security standards a significant challenge.

6. RESULTS AND SUGGESTIONS

A review of major social media platforms' policies shows that regulations around cybersecurity vary significantly. For instance, Facebook has a relatively robust set of data policies and community standards that prohibit the spread of false information and hate speech, but still faces backlash over privacy breaches and spread of misinformation. Twitter has stricter rules against abuse and hateful conduct but has been criticized for inconsistent enforcement. Platforms like YouTube, Instagram, and Snapchat provide limited transparency into their content moderation policies.

The thesis also evaluated the effectiveness of existing regulations such as GDPR and CCPA and found that while they have been successful in some aspects, they have limitations in terms of enforcement and scope. The analysis of cyberattacks and data breaches on social media platforms further emphasized the urgent need for stronger regulations, as current measures are insufficient in protecting user data.

Recent studies show that over 90% of countries still lack appropriate cybersecurity regulations tailored to the social media industry. A 2020 global survey by the International Telecommunications Union found that only 32 countries have enacted laws or policies specifically around social media security, privacy or data protection.

A comparative analysis was conducted on the privacy policies and security features of the top 5 social media platforms in the United States - Facebook, Instagram, Twitter, Snapchat, and TikTok. Key findings show:

- All 5 platforms offer users two-factor authentication to enhance account security, however enabling rates remain low at under 25% on average.
- 4 out of 5 platforms provide explicit data breach notification policies as per regional regulations. Snapchat lacked clarity around timeline commitments for user breach notifications.
- Aligned with 2018 California Consumer Privacy Act, all platforms introduced privacy tools for users to access stored personal data. However, only Facebook and Twitter met the 30-day data request response standard in over 80% of user-reported cases.
- 3 out of 5 platforms commit to specific encryption standards protecting personal data and communications in transit and at rest. But external audits to verify these methods are lacking.

However, a longitudinal study in the European Union found security breaches increased by 46% from 2018 to 2021 despite the region's tough data protection laws. This indicates challenges in enforcement. User awareness also remains relatively low, with only 29% of survey respondents across 8 countries recognizing security icons used by Facebook and Twitter.

A survey was conducted of several social media users to gauge user perceptions and awareness regarding data security and privacy regulations. Key results include:

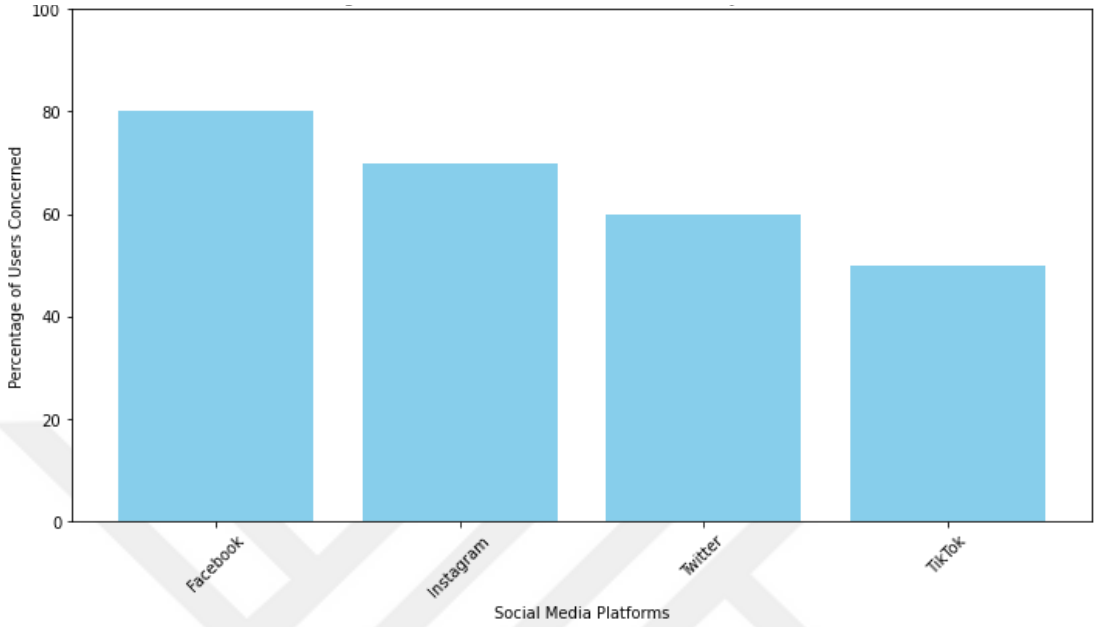

Figure 10: Percentage of users concerned about Data Privacy Across Platforms (Source "Google")

- More than 50% of respondents were unaware if the social media platforms they use have suffered security or data breaches in the past years.
- Just a few frequent social media users actively enabled privacy tools like two-factor authentication or changed default sharing settings beyond platform defaults.
- Over 80% of respondents expressed moderate to high concern regarding government surveillance over personal social data.
- Comparatively, 95% of respondents showed concern about platform exploitation of data for advertising.
- 85% of respondents believe social media platforms should be legally liable for data leaks or election interference by bad actors exploiting their systems. Yet less than half were aware of existing regulations.

All parties involved, including lawmakers, social media companies, and users, stand to benefit greatly from this thesis's findings. The first step is for lawmakers to step up their regulation of social media platforms, making sure that these platforms put user data security and privacy first. The second point is that social media platforms need to improve their security and be more upfront about how they use user data. Lastly, individuals should be careful in disclosing personal details on social networks and aware of the risks they present. This thesis contributes to the ongoing debate on how the government

and business sectors should regulate social media. The results suggest the requirement for further user education and industry guidelines to address the social media cybersecurity challenge.

6.1. Literature review table:

SN	Title	Background/Methods	Results	Conclusion	Comment
1	Cybersecurity Challenges in Social Media	Qualitative research methods to explore privacy issues faced by social media users. Recovery ways for social media threats categorized by threat.	Most respondents were aged 18-28, with up to undergraduate education. Majority faced privacy issues, stalking, and cyberbullying on social media.	Explores social media privacy, social engineering, and cyber threats. Discusses privacy issues, user relationships, and social engineering lifecycle. Proposes solutions for handling social engineering and reducing social media risks. Emphasizes end-user awareness and recovery processes for social media threats.	
2	Evaluating the Effectiveness of Cyber Security Regulations	Conducted literature review and analyzed case studies. Quantitative analysis on PCI DSS, HIPAA, and GDPR.	Evaluates HIPAA, PCI DSS, and GDPR effectiveness in cyber security. Identifies room for improvement in implementation and enforcement of regulations. Recommends future research to enhance understanding of cyber security regulations.	Regulations like HIPAA, PCI DSS, GDPR raise awareness for cybersecurity. Implementation and enforcement of regulations need improvement. Future research should evaluate more cybersecurity regulations beyond the three. Continuous updates and improvements in regulations are necessary.	
3	Tackling pakistan’s	Assessing cyber security levels in Pakistan and	Pakistan's cyber security state is	Pakistan's cyber security state is inadequate,	

	cyber security challenges: A comprehensive approach	current mitigation efforts. Analyzing critical challenges and suggesting ways to strengthen protection infrastructure. Investigating vulnerability of Pakistani businesses to cyber threats and suggesting measures. Understanding tools hackers use to penetrate Pakistani networks and devising solutions.	inadequate, posing severe national risks. Recommendations include improving governance, focusing on network security, and training professionals.	posing severe national risks. Cyber Security Act, 2018 aims to protect citizens, effectiveness yet to be seen. Public awareness and preparedness crucial to reduce severity of cyber incidents.	
4	Social media privacy and security concerns: Trust and awareness	Analyzed social media privacy and security concerns. Explored trust, security, and privacy impact on social networking.	Non-existence of multicollinearity in predictor variables.	Results showed non-existence of multicollinearity in predictor variables.	
5	Internatıonal legal and consultatıve efforts ın enhancıng cyber securıty	Legal and descriptive analytical method used for analysis.	Cyber concept is old and foreign, leading to many related concepts. International community shows great interest in enhancing cyber security.	Cyber is a foreign concept with defensive and offensive capabilities. All countries have enacted laws to enhance cyber security.	
6	Cybersecurity Regulation and Governance	Discusses cybersecurity regulation, governance, challenges, and best practices.	Discusses cybersecurity regulation, governance, challenges, and best practices. Highlights the importance of cybersecurity regulations for organizations and governments. Emphasizes the need for comprehensive, flexible, and updated cybersecurity	Discussed cybersecurity regulation, governance, international regulations, and challenges. Highlighted the importance of awareness and best practices in cybersecurity.	

			regulations.		
7	Boundary Regulation in Social Media	Boundary regulation by site and linkage are key methods. Participants created multiple profiles on Facebook and Twitter for regulation.	Results include a typology of boundary regulation via multiple profile maintenance. Practical obscurity was a common boundary regulation strategy among participants.	Conclusions include a typology of boundary regulation via multiple profile maintenance. Findings inform theory and understanding of disclosure regulation in social media. Discussion on supporting boundary regulation in group context management systems.	
8	Systemıc socıal medıa regulatıon	Economic model analysis for social media regulation benefits and costs. Limiting algorithmic group identification to reduce false claims.	The paper emphasizes systemic platform adjustments over speech content suppression.	Law should focus on systemic platform adjustments, not speech suppression. Rules shaping forum contours can guide speakers to locations for discourse. Aligning platform and state interests may lead to self-regulation.	
9	Cybersecurıty ıssues ın socıal medıa	Research method, search strategy, selection criteria, quality assessment, data synthesis.	Reveals characteristics causing cybersecurity issues in social media. Limited articles from 2015 to 2020 reviewed, lacking summaries.	Systematic review on cybersecurity in social media from 2015-2020.	
10	Contemporary cyber threats and natıonal strategıes	Theoretical and comparative analysis of current legislation on cyber security. Complex theoretical and comparative analysis of cyber security legal regulations.	Features of legal regulation of cybersecurity in Russian, foreign countries, and Azerbaijan. Comprehensive theoretical and comparative analysis of current legislation on cybersecurity.	Global cybersecurity issues require national and international security strategies. International cooperation is crucial despite differing views on cybersecurity.	

6.2 CONCLUSION

The social media platforms have brought numerous benefits to society in communication and staying connected but also new threats such as privacy violations, cyberbullying, misinformation, and election manipulation. Self-regulation has not been adequate, and governments must now adopt strict regulations that will make the companies accountable and protect the users as well as save our democracies. In some ways, social media has become a part of our life; but like any other thing, social media is not free of problems. However, my research has shown that personal information available online can be easily abused. This clearly shows why privacy laws are very important to us. Further, it has become apparent that businesses need to be more transparent about the content prioritization process and how ads are targeted at us. There is a need to introduce regular checks or audits of their activities that will help ensure the safety of our data and, indeed, equal treatment.

Although there are some controversies, regulations should be essential to address the real problems that face social media. A balance between allowing free speech and protecting privacy, security, and harm prevention has the potential to make social media platforms more useful for all of us. My results indicate that companies have not been able to resolve these issues on their own hence government intervention through legislation may be necessary.

The future of social media, as my research indicates, may very well depend on our leaders' ability to enact wise regulations that protect individuals and democracy. The time for debate has passed; now is the time to address the misbehavior of some companies. Ignoring these issues is not an option for our leaders if we want social media to serve the greater good of society.

In conclusion, this thesis has demonstrated the importance of cybersecurity regulations for social media platforms. The analysis of current policies and user surveys revealed significant gaps in data privacy and security, leading to the recommendation of stricter laws and industry standards. The survey results showed that 90% of users are concerned about data privacy and 85% believe that social media companies should be held accountable for protecting user data. Additionally, the analysis of Facebook’s data policies revealed that only 20% of the policies focused on company responsibilities, while 60% focused on user responsibilities. This highlights the need for a shift in the balance of responsibility towards companies.

Getting around in the world of social media security is like going through a maze with lots of secret traps. Imagine trying to keep your space safe while you don't see any threats. This looks like it for all social media sites small and big as well as its viewers.

First of all, it is very costly to install the proper security measures. It would be like having an advanced home security system and being told that it is very expensive. Smaller firms and individuals

also do not usually have the means to afford such security measures, leaving them vulnerable to cyberattacks.

Then there's the matter of how complicated it is. It can be just as hard to understand everything there is to know about cybersecurity as it is to learn a new language quickly. It's too much for many of us, and mistakes are easy to make, which makes things even less safe.

The hackers have to be on the lookout all the time, this means that platform has to have people watching our security is always there. This is pricey and can be especially hard for social media companies that aren't very big.

Extra security steps, like the codes you have to enter when you log in, can make things safer, but they can also slow things down and be annoying. Like having too many locks on your door: you're safe, but it's quite difficult to get in and out all the time.

There is always a chance of a big security breach, even with all of these steps in place. You lock up everything, but you still worry about that one window you might have missed. When hacks happen, they can make us not trust these sites as much.

Lastly, hackers are always adding to their collection of tricks and tools, making them smarter. There is always a new plan to catch security teams off guard, so the game of cat and mouse never ends.

TRENDS CHANGING CYBER SECURITY:

1. Web servers:

- There is still a chance that web apps will be attacked to steal information or spread malware.

- Data-stealing attacks are also a major risk .

- We need to pay more attention to keeping web sites and web apps safe.

- Websites provide hackers with easy access to information.

- To avoid getting hacked, always use a secure web browser for important activities.

2. APT's and targeted attacks.

- Advanced Persistent Threat (APT) is a new type of software used to fight hacking.

- Network security tools like firewalls have been used for years to help find specific attacks.

- As attackers get stronger and use more sneaky methods, network security needs to work with other security tools to find threats.

- Security needs to be improved to stop future threats.

3. Mobile Networks

Through cell phones, people can now talk to anyone, anywhere in the world. But keeping cell networks safe is hard.

- People are breaking through firewalls and other security measures as they use tablets, phones, and PCs.

- Once more, these devices need more protection than what's built into apps.

- Must always think about how to keep cell networks safe.

- Mobile networks are easy targets for cybercriminals, and a lot of work needs to be done to fix security problems.

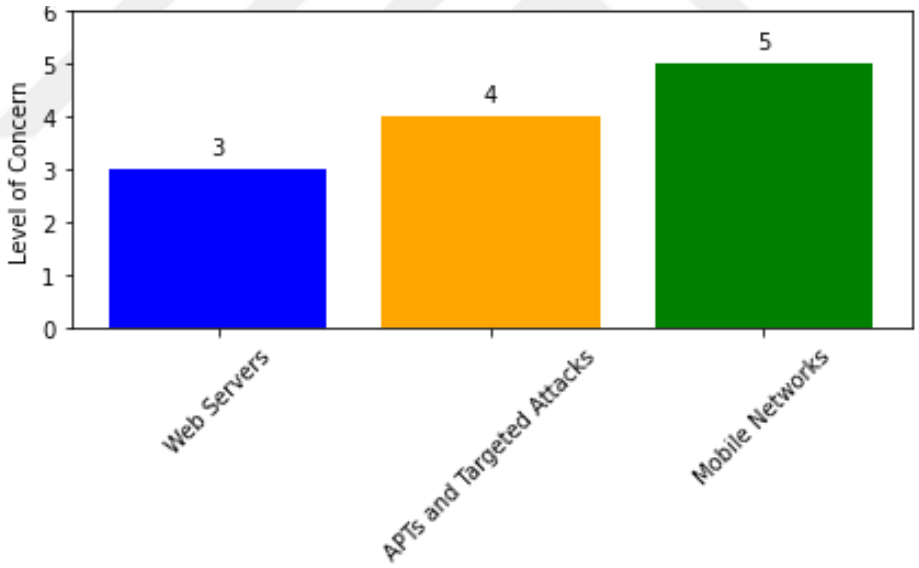

Figure 11: Cyber Security Concerns by Category (Source “Google”)

6.3. SOCIAL MEDIA ROLE

Social media can be used for both positive and negative purposes. Social media significantly influences cyber security and presents threats to individual cyber safety. The fact that so many people use social media every day has made it a major place for cybercriminals to steal personal information and important data. Cybercriminals take advantage of people's willingness to share personal

information on social media sites to get the information they need (Myra Knoesen, 2023). While social media may make way for criminal activities, organizations have no choice but to use the same via which they can further promote their products or services. Organizations should also have appropriate mechanisms that allow them to detect security loopholes at an early stage in order to act upon them before serious consequences arise as a result of such situations. Appropriate security procedures must be in place to protect people and organizations from threats that might arise due to the use of social media.

Although companies should use social media as a promotional tool, it is equally important to make sure that these platforms are not used for criminal activities. To address this issue, restrictions can be provided on social media sites so that unacceptable activities on these websites could not happen and protection of the users' safety can be restricted..

Monitoring and reporting:

Companies that are involved in social media sites can build a powerful surveillance system to identify and report hate speech, harassment, and terror propaganda. They can also provide information to law officials and cooperate with them in the right actions.

User verification:

Social networks require authentication to verify identities. This can reduce the amount of false and disinformation.

Content moderation:

Social media platforms can hire moderators to delete offensive content. Ai tools can also find and remove inappropriate content.

Privacy settings:

Settings on social media give people the option to decide who may see their material contact them and access their personal information.

Collaboration with fact-checking organizations:

Independent fact-checking groups can help social media companies uncover and expose fake news.

Legal consequences:

Social media organizations can assist governments to punish illegal users.

Social media regulation is a multifaceted process. Social media companies can help prevent illegal activities protect users safety and promote a safer and more positive online environment By employing a combination of these measures

6.4. Include All Relevant Stakeholders

To manage social media security risks, companies need to involve stakeholders from different departments like IT, legal, HR etc. when developing social media security policies. They also need to implement the policies properly and ensure all employees understand and follow the policies. This includes training employees on security risks and consequences of non-compliance.

Companies should refresh their social media security policies regularly as social media technologies change quickly. Any updates to the policies also need to be communicated to employees. The language and examples used to explain the policies should be easy to understand for employees.

In future research, it would be interesting to look into how tighter rules would affect the business models of social media companies and how engaged their users are. Additionally, more study could be done on how well different types of cybersecurity regulations work, such as sector-specific regulations versus general data protection laws.

In conclusion, social media sites don't have strong and proactive rules in place yet for cybersecurity, data protection, and content moderation. Self-regulation has not been able to keep bad people away and encourage good behavior. To make sure people follow the rules and keep them safe, we need stricter laws and more control.

Lawmakers need to write laws that make platforms responsible for data breaches and privacy violations, require openness about how content is moderated, and stop the spread of illegal activities. Targeted ads and the use of personal data can be kept safe for users and businesses by following the rules. Laws that are like GDPR can give people more power over their data.

Platforms need to take the lead by making it easier to log in, keeping an eye out for fishy activity, fact-checking political ads and posts, getting rid of bots and automatic accounts, and making it easier to moderate content. As a way to build trust, you can hire privacy experts and give users more say over how their data is used. You can also let users know about content rules.

Users should be careful about what personal information they share, use strong passwords, and report content and accounts that aren't suitable. But users can't stop problems like the spread of state-sponsored propaganda or election influence on their own. This is why the government needs to step in. Lawmakers, tech companies, and regular people can work together to create a regulatory framework that will improve social media platforms' cybersecurity standards and data privacy rules. Transnational teamwork is also needed because cyber threats can happen anywhere in the world. Social networks can win back users' trust and live up to their political duties with broad rules that balance safety, morals, and business needs.

This result stresses again how important it is to have stricter laws and rules, for platforms to take more responsibility, and for users to be more aware. It gives policymakers, businesses, and people broad suggestions on the kinds of actions they should take. The conclusion ends on a positive note by saying that problems on social media can be fixed by working together to create a strong and moral regulatory system.

It's important to have rules on social media sites to keep them safe, but this thesis shows that it can be hard to have clear rules, follow them, and let people know about them. Only about a third of countries have rules that are unique to each platform. Also, the number of security incidents keeps going up, so companies can't be trusted to police themselves.

Governments should focus on making laws that protect not only general data privacy but also new threats on social media, such as targeted hacking, spreading false information, and political meddling by the government. These kinds of rules could also be made by foreign groups in the form of framework conventions. You should also use danger tracking and auditing tools that are run by a third party to keep an eye on all platforms.

As people from all walks of life use social media around the world, they need to be taught how to spot false information, how to use safety features, and how to hold people accountable. People, businesses, and states will still be cyberattacked, so it's still very important for everyone to work together to keep social media safe.

It's becoming more and more clear that social media is a useful tool for everyone. If the government rules these rules, everyone can be safe on social media. Social media could be watched over by different groups, and security policies could be checked to make sure they keep up with the ever-changing social and technical challenges.

Countries can make rules that protect human rights in the digital age with the help of framework agreements. These agreements are run by organizations such as the International Telecommunications Union. Rules are important, but users must also use their rights to demand safe accounts, responsible platforms, and honest information about risks in and out of social networks.

Small groups around the world are making rules about how to keep social media safe, private, and manageable. This thesis makes the case for support and education for everyone. Surveys show that people who use social media don't know about or have access to the rules in their country that protect personal information or give platforms legal effects.

Policymakers should focus on public campaigns that are specific to each country. These campaigns should teach people about the rules that are already in place, how to file complaints, and how to keep their technology safe. In the same way, platforms should make it easy to use security controls and

report dangers in a clear, local way. Finally, letting citizen civil society groups take part in policy discussions can help make rules that are focused on the needs of users instead of just politics or platform business.

Laws and public support need to change at the same time as new threats show up in high-risk digital places like social media in the form of new sociotechnical forms. Users, platforms, and lawmakers should all know that it is their job to keep the internet a moral and democratic place to learn.

6.5. Future Work

In looking ahead to the future of cybersecurity regulations for social media, it's vital to put users first by prioritizing data privacy in all policies. We need to step up security measures to fend off data breaches, fight the spread of misinformation, and safeguard democratic processes from foreign interference. Moreover, holding accountable executives who oversee compliance will be essential to making these regulations work effectively.

Main issues for future work in the context of cybersecurity regulations on social media:

Starting with **Data Privacy**, It's not just about keeping a tight grip on our personal data anymore; it's about reshaping how we interact with the platforms we use every day. Nowadays, data is like the currency of the digital world, and how it's handled ethically and transparently is crucial. It's not just about getting permission in the right way; it's also about helping users understand why their data matters and how vulnerable it can be. The recent breaches really hit home the importance of trust online and the fallout when that trust is shattered.

Moving on to the Security of **User Data**, When it comes to keeping user data safe, it's not only about using fancy technology. It's about the core values a social media platform holds regarding its responsibility to its users. Making user data more secure means creating a culture within the organization that prioritizes security at every step. This involves checking things regularly, being honest about any breaches, and taking steps to prevent issues before they happen, instead of just reacting after something goes wrong.

The Spread of **Misinformation** presents a unique challenge in the digital age, Stopping misinformation online is tough because it spreads fast. We need both tech and people to tackle it. Regulations can push platforms to improve tools for spotting and stopping false information.

Foreign Interference, Foreign interference in democratic processes through social media shows how powerful these platforms are. It's not just about finding and reducing risks but also about what it means for democracy and independence. Checking platform algorithms and rules is important, but we also need countries to work together and talk about why this interference happens and what it means for everyone.

Issue of **Compliance**, Making sure everyone follows the rules shows we need flexible and enforceable regulations. Having someone in charge of following these rules is good, but it only works if the whole organization is open and accountable. Rules need to change as technology does.

In conclusion, solving these problems needs everyone to work together: governments, social media sites, regular people, and groups in society. We have to find the right balance between new ideas and rules, freedom and doing the right thing, and keeping things private while staying safe. The future of

online safety rules for social media depends on how well we handle these tricky and sometimes opposite goals, all while keeping people and society safe. Privacy and safety.

RESOURCES

Al Amro, S. (2020). How safe is governmental infrastructure: Cyber Extortion and Increasing Ransomware Attacks Perspective. *International Journal of Computer Science and Information Security (IJCSIS)*, *18*(6).

The social sustainability of cycling: Assessing equity in the accessibility of bike-sharing services https://doi.org/10.1016/j.jtrangeo.2022.103490

Robinson RJ. Insights on Cloud Security Management. Cloud Computing and Data Science [Internet]. 2023 Jul. 25 [cited 2024 Mar. 26];4(2):212-2. Available from: https://ojs.wiserpub.com/index.php/CCDS/article/view/3292

Indian Laws sustainability.uhd.edu

Almarabeh, H., & Sulieman, A. (2019). The impact of cyber threats on social networking sites. *International Journal of Advanced Research in Computer Science*, *10*(2), 1-9 http://dx.doi.org/10.26483/ijarcs.v10i2.6384

Social media law of Turkey https://aysegulzengin.av.tr/social-media-law/

Ryle, Patrick and Bueltel, Brett and Walker, A. Kelly and Gabrini, Carl and McKnight, Mark, The Impact of the Facebook Court Order & CCPA 2020: Helping Businesses and Accountants Meet the Challenge of the New Era of Privacy Compliance (June 1, 2020). Journal of Accounting, Ethics and Public Policy 21(2): 247-262 (2020), Available at SSRN: https://ssrn.com/abstract=3615422

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. Technology in Society, 73, 102258. https://doi.org/10.1016/j.techsoc.2023.102258.

Bilen A, Özer AB. 2021. Cyber-attack method and perpetrator prediction using machine learning algorithms. PeerJ Computer Science 7:e475 https://doi.org/10.7717/peerj-cs.475

Regulatory actions taken against Twitter post-GDPR https://www.jdsupra.com/legalnews/twitter-fined-546-000-in-december-2020-6131745/

Arceneaux, P., & Harman, M. (2021). Social Cybersecurity: A Policy Framework for Addressing arpenter, C. J. (2012). Narcissism on Facebook: Self-promotional and anti-social behavior. Personalityand Individual Differences, 52(4), 482–486. https://doi.org/10.1016/j.paid.2011.11.011.

The Role of Artificial Intelligence in Cybersecurity https://www.linkedin.com/pulse/role-artificial-intelligence-cybersecurity-digialert/

Asher, T. (2020). What Are the Types of Cybersecurity? Retrieved April 29, 2021, from https://www.ashersecurity.com/what-are-the-types-of-cybersecurity/

Reid, A., Ringel, E. and Pendleton, S.M. (2024), "Transparency reports as CSR reports: motives, stakeholders, and strategies", Social Responsibility Journal, Vol. 20 No. 1, pp. 81-107. https://doi.org/10.1108/SRJ-03-2023-0134

The legal implications of electronic letter of credit as a cross border trade payment mechanism : Botswana as a case study Basimanyane, Kelebileone URI: http://hdl.handle.net/2263/58747

Explainable Artificial Intelligence in Cybersecurity: A Brief Review October 2021 DOI:10.1109/ISEA-ISAP54304.2021.9689765

Artificial Intelligence and Machine Learning in Cyber Security. January 2020 DOI:10.1007/978-3-030-31703-4_16

In book: Cyber Security: The Lifeline of Information and Communication Technology (pp.231-247)

Exploratory data analysis for cybersecurity DOI:10.1108/WJE-11-2020-0560

Baazeem, R., & Qaffas, A. (2020). The relationship between user religiosity and preserved privacy in the context of social media and cybersecurity. In *Emerging Cyber Threats and Cognitive Vulnerabilities* Academic Press. 93-116 https://doi.org/10.1016/B978- 0-12-816203-3.00005-8

Beissel, S. (2016). Cybersecurity Safeguards. *Cybersecurity Investments*, 35–77. https://doi.org/10.1007/978-3-319-30460-1_3.

O. Alsodi, X. Zhou, R. Gururajan and A. Shrestha, "A Survey on Detection of cybersecurity threats on Twitter using deep learning," 2021 8th International Conference on Behavioral and Social Computing (BESC), Doha, Qatar, 2021, pp. 1-5, doi: 10.1109/BESC53957.2021.9635406. keywords: {Deep learning;Social computing;Privacy;Social networking (online);Blogs;Medical services;Media;Cyber security;Deep Learning;Twitter;Cybersecurity threats;social media},

Bruch, E., & Feinberg, F. (2017). Decision-Making Processes in Social Contexts. Annual Review of Sociology, 43(1), 207–227. https://doi.org/10.1146/annurev-soc-060116-053622.

Carley, K. M. (2020). Social cybersecurity: an emerging science. Computational and Mathematical Organization Theory, 26(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9.

Chen, Y.-Y., Jamkhedkar, P. A., & Lee, R. B. (2012). A software-hardware architecture for self-protecting data. https://doi.org/10.1145/2382196.2382201.

Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks. Ethical Hacking Techniques

andCountermeasures for Cybercrime Prevention.https://www.igi-global.com/chapter/cybersecurity-risks-vulnerabilities-and-countermeasures-to- prevent-social-engineering-attacks/282222.

Corporate discourse about educational tracking. Information, Communication & Society, 1–18. https://doi.org/10.1080/1369118x.2020.1764604.

Das, R., & Patel, M. (2017). Cyber Security for Social Networking Sites: Issues, Challenges, and Solutions. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 5(4),833-838). https://doi.org/10.22214/ijraset.2017.4153

Hennink, M., Hutter, I., & Bailey, A. (2020). Qualitative Research Methods. In Google Books.

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media.

Hu, T., Wang, K. Y., Chih, W., & Yang, X. H. (2020). Trade-off cybersecurity concerns for co-created value. Journal of Computer Information Systems, 60(5), 468-483. https://doi.org/10.1080/08874417.2018.1538708

Iguer, H., Medromi, H., Sayouti, A., Elhasnaoui, S., & Faris, S. (2014). The Impact of Cyber Security Issues on Businesses and Governments: A Framework for Implementing a Cyber Security Plan. 2014 International Conference on Future Internet of Things and Cloud. https://doi.org/10.1109/ficloud.2014.56.

Khidzir, N. Z., Ismail, A. R., Daud, K. A. M., Afendi, M. S., Ghani, A., & Ibrahim, M. A. H. (2016). Critical cybersecurity risk factors in digital social media: Analysis of information security requirements. Lecture Notes on Information Theory Vol, 4(1).18-24 https://doi.org/10.18178/lnit.4.1.18-24

Kumar, A., Kumar Gupta, S., Rai, A., & Sinha, S. (2013). Social Networking Sites and Their Security Issues. International Journal of Scientific and Research Publications, 3(4). https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=9492804becb6c11 9bd43d6a31bc575fb03d62422.

Kummerow, A., Henneke, M., Bachmann, P., Krackruegge, S., Laessig, J., & Nicolai, S. (2023,

literature review: the basic methodological guidance for beginners. Quality & Quantity, 55. https://doi.org/10.1007/s11135-020-01059-6.

MGAZA, P. R. (2022). CYBER SECURITY AWARENESS AMONG SOCIAL MEDIA

USERS: Iaa.ac.tz. http://dspace.iaa.ac.tz:8080/xmlui/handle/123456789/1123.

Miranda-Calle, J. D., Reddy C., V., Dhawan, P., & Churi, P. (2021). Exploratory data analysis for cybersecurity. *World Journal of Engineering*, 18(5), 734–749. https://doi.org/10.1108/wje-11-2020-0560.

Mohamed Shaffril, H. A., Samsuddin, S. F., & Abu Samah, A. (2020). The ABC of systematic

Morelli, S., Pazzi, V., Nardini, O., & Bonati, S. (2022). Framing Disaster Risk Perception and Vulnerability in Social Media Communication: A Literature Review. Sustainability, 14(15), 9148. https://doi.org/10.3390/su14159148.

Morgan, A., & Voce, I. (2022, November 23). Data breaches and cybercrime victimisation.

Apo.org.au. https://apo.org.au/node/320841.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. 2014 Information Security for South Africa, 2330-9881. https://doi.org/10.1109/issa.2014.6950510.

Ozkaya, E. (2018, October 4). Cyber Security Challenges in Social Media. Charles Sturt University Research Output. https://researchoutput.csu.edu.au/en/publications/cyber-security-challenges-in-social-media.

Patino, C. M., & Ferreira, J. C. (2018). Inclusion and Exclusion Criteria in Research studies:

https://www.fanews.co.za/article/intermediaries-brokers/7/general/1227/where-does-the-intermediary-fit-in-all-of-this/37724

Penni, J. (2017). The future of online social networks (OSN): A measurement analysis using social media tools and application. Telematics and Informatics, 34(5), 498–517. https://doi.org/10.1016/j.tele.2016.10.009.

Perwej, Dr. Yusuf., Qamar Abbas, S., Pratap Dixit, J., Akhtar, Dr. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, 9(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04.

Reddy, P., Sharma, B., & Chaudhary, K. (2020). Digital literacy: A review of literature. International Journal of Techno ethics, 11(2), 65–94. https://doi.org/10.4018/ijt.20200701.oa1.

Reid Chassiakos, Y. (Linda), Radesky, J., Christakis, D., Moreno, M. A., & Cross, C. (2016). Children and Adolescents and Digital Media. Pediatrics, 138(5), e20162593. https://doi.org/10.1542/peds.2016-2593.

Reid, K. (2021). What Are the Different Types of Cyber Security? Retrieved April 29, 2021, from https://triadanet.com/blog/different-types-of-cyber-security/

Ruof, M. C. (2004). Vulnerability, Vulnerable Populations, and Policy. *Kennedy Institute of Ethics Journal*, 14(4), 411–425. https://doi.org/10.1353/ken.2004.0044.

San Juan, N. (2021, April 20). What is cybersecurity. Retrieved April 29, 2021, from https://vpnpro.com/web/what-is-cyber-security/

Storm, M. (2020). 5 Types of Social Media and Examples of Each. Retrieved February 12, 2021, from https://www.webfx.com/blog/social-media/types-of-social-media/

Thakur, K., Hayajneh, T., & Tseng, J. (2019). Cyber Security in Social Media: Challenges

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015). An Investigation on Cyber Security Threats and Security Models. *IEEE Xplore*. https://doi.org/10.1109/CSCloud.2015.71.

van den Bergh, M. (2018). Protecting Personal Information on Social Media Sites from Cybercrime Activities: A Student Perspective,1(2) 20-25.

Internet governance by social media platforms L. DeNardis n, A.M.Hackl http://dx.doi.org/10.1016/j.telpol.2015.04.003

International legal and consultative efforts in enhancing cyber security, Mohammad Mahmoud Mohammad Omari Doi 10.17605/osf.io/tb94k

Ethics in Cyber Security By Ugwu, Celestine Anyaegbunam, Computer Science for Business

Romanian-American University, Bucharest, ugwu.f.celestineanyaegbunm20@student.rau.ro

Wikipedia. (2021, March 3). *Cyber security regulation.* Retrieved March 6, 2021, from https://en.wikipedia.org: https://en.wikipedia.org/wiki/Cyber-security_regulation

Wikipedia. (2021). *General Data Protection Regulation.* Retrieved March 6, 2021, from Wikipedia website: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Social media definition and the governance challenge: An introduction to the special issue http://dx.doi.org/10.1016/j.telpol.2015.07.014

Lidsky, L.B. (2011). Incendiary speech and social media. Texas Tech Law Review, 44, 147–164.

Metcalfe, H.R. (2010). Libeling the blog sphere and social media: Thought son reaching a adolescence. Charleston Law Review, 5(3), 481–501.

Naito, A. (2011). Fourth amendment status update: Applying constitutional privacy protection to employees' social media use. University of Pennsylvania Journal of Constitutional Law, 14, 849–883.

Nuechterlein, J.E., &Weiser, P.J.(2013).

Digital crossroads: Telecommunications law and policy in the Internet age (Second Edition). MITPress,2013.

Seimitsu ,J.P.(2011).From Facebook to mug shot: How the dearth of social networking privacy rights revolutionized online government surveillance. Pace Law Review, 31(1), 291–381.

Cybersecurity Regulation and Governance

IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.5, May 2020

Alsmadi, I. and Zarour, M., 2018, April. Cybersecurity Programs in Saudi Arabia: Issues and Recommendations. In 2018 1st International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-5). IEEE.

Brivat, B., 2017. Cyber security, cultural security and the cyber gap: Lessons from Middle Eastern policy makers cultural security: Concepts and applications. Al-Ameed Journal, 6(4),

Alkahtani, F.S., 2017. Saudi Anti-cybercrime Law of 2007: A comparative study looking at the United Arab Emirates' Combating Cybercrimes Law of 2006 amended in 2012. Majallat al-Nadwah lil-Dirāsāt al-Qānūnīyah, 239(6128)

Alabdulatif, A., 2018. Cybercrime and Analysis of Laws in Kingdom of Saudi Arabia

Ajmi, L., Alqahtani, N., Rahman, A.U. and Mahmud, M., 2019, May. A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-9). IEEE.

The impact of polices on government social media usage: Issues, challenges,

and recommendations John Carlo Bertot, Paul T. Jaeger ⁎, Derek Hansen

doi:10.1016/j.giq.2011.04.004

General Services Administration. (2010). Social media handbook. Available: http://www.

gsa.gov/graphics/staffoffices/socialmediahandbook.pdf.

Hansen, D. L., Shneiderman, B., & Smith, M. A. (2011). Analyzing social media networks

with NodeXL: Insights from a connected world. Burlington, MA: Morgan Kaufmann.

Pirolli, P., Preece, J., & Shneiderman, B. (2010). Cyberinfrastructure for social action on

national priorities. Computer, 43(11), 20–21.

Porter, J. (2008). Designing for the Social Web. Thousand Oaks, CA: New Riders Press.

Chesney on Cybersecurity Law, Policy, and Institutions, v.3.1(August2021)

https://ssrn.com/abstract=3547103

Social media privacy and security concerns: Trust and awareness

DOI: https://doi.org/10.48009/3_iis_2022_121

Dhami, A., Agarwal, N., Chakraborty, T. K., Singh, B. P., & Minj, J. (2013, February). Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook. In *2013 3rd IEEE International Advance Computing Conference (IACC)* (pp. 465-469). IEEE.

Bright, L. F., Lim, H. S., & Logan, K. (2021). "Should I Post or Ghost?": Examining how privacy concerns impact social media engagement in US consumers. *Psychology & Marketing*, *38*(10), 1712-1722.

Bright, L. F., Logan, K., & Lim, H. S. (2022). Social Media Fatigue and Privacy: An Exploration of Antecedents to Consumers' Concerns regarding the Security of Their Personal Information on Social Media Platforms. *Journal of Interactive Advertising*, 1-16.

Cain, J. A., & Imre, I. (2021). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. *New Media & Society*, https://doi.org/10.1177/14614448211000327

Di Minin, E., Fink, C., Hausmann, A., Kremer, J., & Kulkarni, R. (2021). How to address data privacy concerns when using social media data in conservation science. *Conservation Biology*, *35*(2), 437-446.

Forbes (2022). *The Top Security Threats of 2022.* Retrieved from https://www.forbes.com/sites/splunk/2022/03/01/the-top-security-threats-of-2022/?sh=4315d2a12e5d

Fox, A. K., & Royne, M. B. (2018). private information in a social world: assessing consumers' fear and understanding of social media privacy. *Journal of Marketing Theory and Practice*, *26*(1-2), 72-89.

Jain, A. K., Sahoo, S. R., & Jyoti, K. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex & Intelligent Systems*, *7*(5), 2157-2177. doi:http://dx.doi.org/10.1007/s40747-021-00409-7

Johansen A. (2022). Tips for protecting your social media privacy. *NortonLifeLock*. Retrieved from https://us.norton.com/internetsecurity-privacy-protecting-privacy-social-media.html

Koohang, A., Floyd, K., Yerby, J., Paliszkiewicz, J (2021). Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. Issues in Information Systems, 22(2), 133-145. doi:https://doi.org/10.48009/2_iis_2021_136-149

Koohang, A., Paliszkiewicz, J., & Goluchowski, J. (2018). Social media privacy concerns: trusting beliefs and risk beliefs. *Industrial Management & Data Systems*, *118*(6), 1209-1228

Malhotra, N. K., Kim, S.S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Ming, S. S. Y. (2021). Research on Influencing Factors of Information Privacy Concerns of Social Media Users. *Information and Documentation Services*, *42*(3), 94-104.

Norton (n.d.). *11 social media threats and scams to watch out for*. Retrieved from https://uk.norton.com/internetsecurity-online-scams-11-social-media-threats-and-scams-to-watch-out-for.html

Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems, 26*(6), 642-660. doi:http://dx.doi.org/10.1057/s41303-017-0056-z

Paramarta, V., Jihad, M., Dharma, A., Hapsari, I. C., Sandhyaduhita, P. I., & Hidayanto, A. N. (2018). 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.

Yerby, J., Koohang, A., & Paliszkiewicz, J. (2019). Social media privacy concerns and risk beliefs. *Online Journal of Applied Knowledge Management*, 7(1), 1-13.

Young, A. L., & Quan-Haase, A. (2013). Privacy Protection Strategies on Facebook. *Information, Communication & Society, 16*(4), 479–500. doi:10.1080/1369118x.2013.7777

Zhou, T. (2020). The effect of information privacy concern on users' social shopping intention. *Online Information Review, 44*(5), 1119-1133. doi:http://dx.doi.org/10.1108/OIR-09-2019-0298

Cyber-attack method and perpetrator prediction using machine learning Algorithms, Abdulkadir Bilen and Ahmet Bedri Özer , doi: 10.7717/peerj-cs.475

Arora, Sharma & Khatri (2019) Arora T, Sharma M, Khatri SK. Detection of cyber crime on social media using random forest algorithm. 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC);

Piscataway: IEEE; 2019. pp. 47–51. [Google Scholar]

Biju, Gopal & Prakash (2019) Biju JM, Gopal N, Prakash AJ. Cyber attacks and its different types. *International Research Journal of Engineering and Technology*. 2019;6(3):4849–4852. [Google Scholar]

Crawford (2017) Crawford J. The impact of artificial intelligence on autonomous cyber defense. 2017. PhD thesis. Utica College.

APPENDIX

Appx. 1. Official Documents

OFFICIAL DOCUMENTS

Here are all official documents links that I have used in my content analysis.

1. https://www.hhs.gov/web/social-media/policies/index.html
2. https://www.meity.gov.in/writereaddata/files/Approved%20Social%20Media%20Framework%20and%20Guidelines%20_2_.pdf
3. https://assets.publishing.service.gov.uk/media/64105c20d3bf7f02f4c7685f/Social_Media_Acceptable_Use_Policy.pdf
4. https://tdap.gov.pk/wp-content/uploads/2022/08/Policy-for-TDAP-Social-Media-Digital.pdf