

Investigative Analysis on Accessibility of User Data through Privacy Policy Statement of Leading Web Platforms

Tanika Sharma*, B. Sundaravadvazhagan**

*Analyst, Strategy, Analytics and M&M Advisory, Deloitte. Email: tanikasharma542@gmail.com

**Professor, Department of Information and Technology, University of Technology and Applied Sciences-Al Mussana, Oman. Email: sundaravadi@act.edu.com

Abstract—A privacy policy is nothing more than a legal document for a website. It describes the company's specifics, visitors' perspectives on the data, and establishment methods. It is an essential component of every website, and firms need to ensure that it is factual and understandable even to laypeople. Continuous data collection from data subjects through digital infrastructure is a widespread practice involving numerous stakeholders. This presents significant concerns regarding data protection and user privacy. The main objective of a privacy statement is to inform us about handling personal information acquired during the visit to a website/mobile application. Many Platforms make use of this privacy policy for their business development. Here we analyse the privacy policy of the leading brands and the economy from our user data. This article aims to provide awareness to the user about the usage of his data with his concern.

Keywords—Web Platforms, Privacy Policy, Facebook, Meta, Google, Twitter, Security, User data, User consent, Policy

I. INTRODUCTION

It is a common practice to accept the privacy policy without reading it while downloading a new app or creating a new online account. Many businesses collect a significant amount of personal information and may share it. In an article by Jennifer Schlesinger and Andrea Day of CNBC, privacy professionals disclosed a lot of information about the privacy policies of leading corporate brands. They listed three main points:

1. The typical Person with average education finds these policies complex.
2. They are not created to be understood by consumers.
3. Lawyers, on behalf of the company, develop them to protect their interests.

Reading an average privacy policy by a leading brand takes more than 30 minutes of time and requires a minimal understanding from grade 12 to advanced degrees. Leading brands like Google, Facebook, and Instagram offer their services for free. In exchange, the customers are providing these companies with their data. Leading cyber security

analyst Brian Vecchi, the field chief technology officer for Varonis, has agreed that "Unless you've paid for it, you're the product". This suggests that if a service or product is free, it often means that the data, attention, or personal information is being used or monetized in some way by the provider. According to Vecchi, many policies contain wordings stating that a corporation may modify the policy at any moment without prior notification. However, companies should not be allowed to change their privacy policy without alerting people. Without an individual's permission, businesses should not be allowed to start gathering additional data about them. Many companies monetize the information gathered from individuals by selling it to third parties.

Countries worldwide are recognizing the importance of safeguarding their citizens' data and privacy (Pandey et al., 2020). Now the governments are starting to control how businesses collect data. Last year, the General Data Protection Regulation took effect in Europe, mandating that businesses collecting data in European Union member states update their consumer-facing policies. The General Data Protection Regulation of the European Union went into effect on May 25, 2018. The policy was primarily created to establish stricter guidelines for using

and sharing personal data and to increase transparency in how businesses manage personal data.

The Pew Research Center chose to examine the individual privacy policies of the most popular websites on the Internet to compare word count, reading duration, and reading level before and after GDPR, to assess how easily people could understand these businesses' policy modifications. The implementation of the General Data Protection Regulation (GDPR) in Europe has not only prompted businesses to update their data policies but has also heightened the importance of cybersecurity measures to safeguard personal data in an era of increased data regulation and transparency. According to Neeladri Shekhar Dutta, organizations are exposed to various kinds of risk situations and factors due to the enablement of digital businesses, both during and after digital transformation (Dutta, 2020). It would be difficult for these risks to be handled and detected by using the conventional and existing security practices for IT.

Google processes over 40,000 search queries each second, totalling approximately 3.5 billion daily searches. The volume of raw data acquired by Google is staggering, considering that search is just one way for the company to obtain information from consumers. Some estimates place Google's data storage at around 15 exabytes. To put things in perspective, one exabyte is equivalent to one million terabytes. Due to the sheer volume of users and data, Google is more vulnerable to data breaches. It might not surprise you that Google's privacy policy increased by more than 48% due to the GDPR. Fig. 1 below depicts the changes in privacy policy before & after GDPR.

Privacy Policy Before GDPR				Privacy Policy After GDPR			
COMPANY	WORD COUNT	READING TIME*	READING LEVEL	COMPANY	WORD COUNT	READING TIME*	READING LEVEL
Google	2722	12.54	14	Google	4056	19.81	14
Facebook	5420	26.24	11	Facebook	4233	20.41	13
Reddit	1524	26.42	12	Reddit	3414	16.39	12
Amazon	2627	12.48	12	Amazon	5837	18.24	13
Wikipedia	2881	13.49	15	Wikipedia	5677	27.06	14
Yahoo	1611	7.44	14	Yahoo	2225	11.12	15
Twitter	3764	18.57	15	Twitter	4880	22.25	15
eBay	5244	25.27	18	eBay	5666	27.32	20
Instagram	2981	14.26	12	Instagram	4221	20.38	13
Netflix	3046	15.10	15	Netflix	3477	16.39	16

Fig. 1: Changes in Privacy Policy Before & After GDPR

Mark Zuckerberg testified before Congress and the European Parliament after facing robust public scrutiny in the wake of the Cambridge Analytica controversy. Following his testimony, the head of the European Parliament's Civil Liberties, Justice, and Home Affairs

Committee remarked, 'Mr. Zuckerberg and Facebook will have to make significant efforts to persuade individuals that Facebook fully complies with European data protection rules.' How successful were Facebook's attempts to make its privacy policy more readable in light of the GDPR? The reading level increased by two full grades, despite a reduction in reading time of over 5 minutes. The GDPR has implemented enough measures to prevent the exploitation of user data. Still, multiple corporate brands are penalized with fines for their privacy breaches in the name of the privacy policy. In this article, we explore the privacy policy of each brand and the data collected by each platform through their privacy policy statements.

II. LITERATURE REVIEW

The proliferation of social media platforms has led to an increased reliance on Privacy policies to govern the handling and security of user information. Paradoxically, in a society where personal data becomes more accessible to the general public, the demand for privacy remains strong. Individuals often misconceive their ability to control the extent of personal information made public, believing they can determine who accesses it and how it is used. This complex interplay of privacy and public data impacts nearly every aspect of an individual's life and society at large, rendering privacy a multifaceted and challenging concept to define. This paper explores the intricate relationship between privacy policies, privacy concerns, and security measures on social media platforms (Rewaria, 2021).

A. Privacy Policies of the Web Platform

As numerous enterprises have increasingly inhabited the Internet, many studies have focused on privacy regulations. (Graber et al., 2002) investigated the privacy policies of 80 different Internet health websites. S.D. Lewis opted to examine 75 different internet firms in the banking industry. Analysing how readable the privacy regulations were, was the primary goal of this research. The researchers came to a conclusion in both cases that these groups' privacy rules were complex for most users to understand and were not seen as an effective way to notify users of their privacy rights (Lewis, Colvard & Adams, 2008). One of the few attempts that got the closest to our goals in this work was that of (Caramujo & Da Silva, 2015), who concentrated on Facebook and LinkedIn. However, they did not research other well-known websites like Google and Twitter, nor did they

thoroughly examine their privacy policies. Their approach was centred on the creation of a privacy-aware unified modelling language profile based on privacy policies. Despite these efforts, challenges persist in enhancing privacy and security in social media platforms.

B. Possible Threats and Privacy Risk in Social Network Sites

The use of social networking sites exposes users to a range of concerns, with privacy invasion being the most prevalent. Research has shown that privacy can be infringed upon in several ways, particularly when personal data is not effectively and consistently used. Security may be compromised if unauthorized access to user data occurs, stemming from a privacy breach or improper data handling strategies. The optional use of gathered information for different purposes without the user's knowledge or consent can also result in privacy violations. However, the implementation of relevant information rules and practices that provide users with greater control over their data disclosure can help mitigate many of these security issues.

Users can exercise control over their data sharing based on their goals, knowledge, and security awareness by utilizing disclosure mechanisms. Online social interactions may enforce limit restrictions through privacy settings (Van Eecke & Truyens, 2010), enhancing individuals' capacity to share information while ensuring access to relevant settings.

C. IUIPC - Internet Users' Information Privacy Concerns

Internet Users' Information Privacy Worries (IUIPC) is a model that summarises internet users' concerns about the confidentiality of personal information. Concerns for Information Privacy (CFIP) model (Stewart & Segars, 2002) was developed by the IUIPC model to bring people's attention to organizational information confidentiality processes. The IUIPC model is then constructed by connecting these three aspects, namely beliefs in trust, perceptions of risk, and intentions regarding behaviour, as distinct components of the concept of trust (Malhotra et al., 2004). To be deemed fair regarding information privacy, S.C.'s theory proposes that gathering personal information from social media provider platforms allows users choice over that information and educates users about the company's planned use of the gathered data. As a result, Malhotra defines IUIPC as Internet users'

worry about gathering personal information via social media, the users' control over the information that has been gathered, and the users' understanding of how the obtained information is maintained.

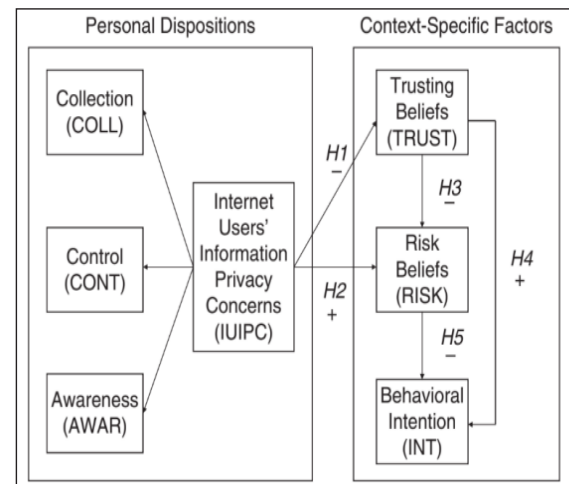


Fig. 2: IUIPC Model

Sipior re-evaluated the IUIPC concept and assumptions to determine its continuous relevance (Sipior et al., 2013), as seen in Fig. 2. According to a previous study, another constant finding is that, as the confidence of people in an online platform grows, individuals are less inclined to view disclosure of personal information as unfavourable (H3) (Malhotra et al., 2004). One more constant finding is that, as trust in an online platform increases, so does the likelihood of the individuals sharing confidential information online (H4).

Finally, the greater the danger of consumers sharing personal information online, the less likely they are to do so (H5). Nonetheless, the IUIPC theory did not exhibit a negative correlation with user confidence in an online platform (H1) but showed a positive correlation with the user's inclination to take risks when sharing private information with an online platform (H2). These findings point to the complexity of user behaviours and the interplay of factors that influence privacy-related decisions.

III. RESEARCH METHODOLOGY

This literature review emphasized leading web platforms' privacy concerns, particularly in terms of user privacy control and knowledge. The researcher initially establishes a research question before locating and selecting relevant prior research studies, technical papers, press releases, and news articles on the subject. The evaluation covers reports that have been released since 2010.

In this research, the first step was to analyse the privacy policy statements of different web platforms, and the research target is popular web platforms like Meta, Twitter, and Google.

Google has faced longstanding criticism for its data collection practices involving internet users, its invasive tracking methods, and the extensive data it shares with governments. However, Google Analytics has recently become one of the most significant privacy issues. The Austrian Data Protection Authority's (DPA) decision on December 22, 2021, represents the first concrete European move against Google Analytics, further intensifying the ongoing debate. This decision underscores the urgency for new EU-US data legislation.

Google, one of the businesses frequently criticized for violating customers' privacy, has made an effort to reassure customers. It pledged to put an end to third-party cookie tracking and introduced more user-friendly controls for individuals to disable their location and internet histories within the company's platform, provided an Android toggle to anonymize your data and prevent businesses from accessing it, and even introduced steps like Federated Learning of Cohorts (FLoC). However, the latter has also drawn much criticism, with privacy groups criticizing Google for simultaneously intensifying user surveillance and monopolizing the market. With this and the most extensive anti-competition inquiry still open for Google, the company has now released an FAQ sheet outlining the "most requested" privacy issues and its responses.

Meta, the data-hungry advertising giant, gathers substantial amounts of your data. Due to regulatory scrutiny and whistle-blowers' claims, the social network has been under intense pressure for the past few months. The privacy modifications made by Apple, which might cost Facebook \$12 billion, complete the perfect storm facing the social network headed by Mark Zuckerberg.

In a blog post detailing updates to its privacy policy, Meta asserts that there have been no alterations. However, the social media company will now furnish more comprehensive information about the data it collects and the parties receiving it. This is beneficial, given that Meta has not consistently been transparent about data destinations.

The Facebook privacy change gives users a greater control over who sees their posts and affects Facebook, Instagram, and Messenger but not WhatsApp (Jansson &

Christensen, 2016). On Twitter, privacy differs from other platforms. The purpose of social media is often for users to publish items publicly for others to see, like, comment on, and retweet. Concerns regarding user privacy on the platform should also be raised in light of a whistleblower's charges that the firm deceived authorities about shoddy security and spam. Like most other social media networks, Twitter relies on advertising and user data access for revenue generation. Users can adjust settings to mitigate some data-sharing activities, but complete cessation is challenging.

IV. DATA ANALYSIS AND FINDINGS

A. Google

The most widely used and famous search engine worldwide is Google. With only a few critical terms entered into a famous Internet search engine like Google, anyone can easily search for any information online and instantly have it at their fingertips.

Methodology: Previous and current privacy policies must be gathered in order to analyse Google privacy standards throughout time. The most recent version of Google's privacy statement may be seen on its website, but older statements can be found through the Internet Archive, better known as the Wayback Machine.

Results: The initial discovery from our study indicates that the clarity of Google's privacy policies has notably declined.

The reading grade level of the policies is one indicator of difficulty. As seen in Fig. 3, Google's privacy policies have always had a high reading grade level. Although the reading grade level has decreased marginally over the years, the expectation remains at or above the 12th-grade level.

As per the Clear Language Group, "text should be produced at the eighth-grade level or below for the general population." The readability index of online consumer health sites was determined to be 10.5. According to Google's "Finding Your Way Around YouTube" standards, just a Flesch-Kincaid reading grade level of 9.3 is necessary. Google seems to be enhancing the accessibility of its privacy policies for the general public by incorporating more video explanations and visual elements within its existing privacy policy documents. (Peslak et al., 2020a).

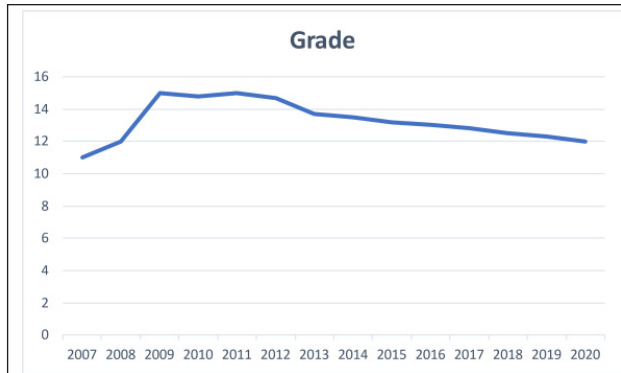


Fig. 3: Reading Grade Level

The rising complexity related to the Google's privacy policy is mirrored in the word count (see Fig. 4). In 2000, the privacy policy had a word count of 657, with little more than one page of information. In 2009, the word count increased to 2,140 on four pages. Since 2000, personal information options, information sharing, information security, data integrity, accessing and updating personal information, and enforcement have all been covered. Additionally, back in the year 2000, sections like "What Information Do We Collect" and the "Google and Cookies" sections contained three paragraphs, which have since expanded to fourteen paragraphs.

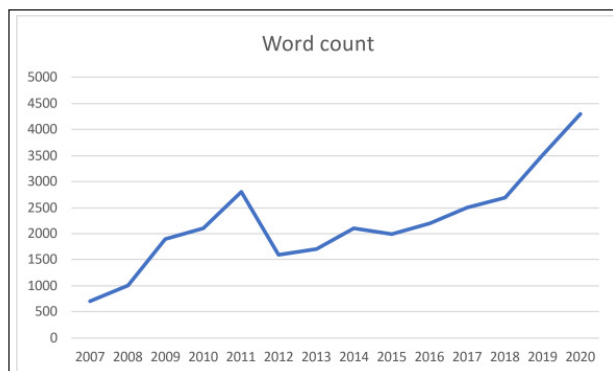


Fig. 4: Word Count

Then we assess the analytical scores of the different Google privacy policies. A strong analytical score indicates a tendency toward structured, rational, and systematic thinking, while a low score indicates a preference for informal and subjective thinking (Peslak et al., 2020b). In Figure 5, there is a notable decrease in the analytical score between the years 2011 and 2012, coinciding with the introduction of a more personalized user experience. Google began utilizing the phrases "you," "your," and "our users" to provide a more personalized experience.

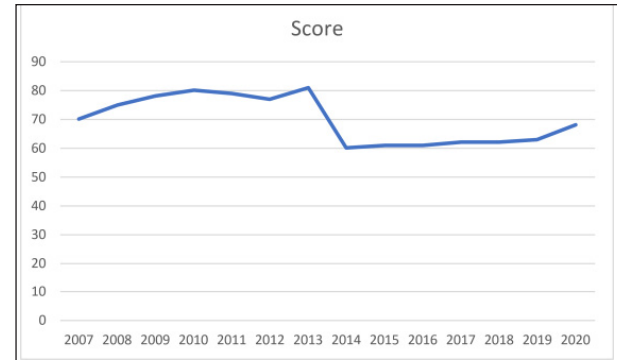


Fig. 5: Analytic Scores

It has been observed that, with the exception of one year, authenticity ratings declined dramatically during the 18 years, indicating a more conservative, legalistic, and less personal attitude. The score was 48.0 in 2000; it rose to 51.1 in 2004 and then dropped to 19.4 in 2018, the year with the most recent privacy policy. In addition to "we create and administer our services with the protection of your privacy in mind," they added, "our" and "your" in 2004. This is most likely responsible for the minor rise in numbers.

B. Meta

Meta revised the Privacy Policy in response to Meta users' and privacy experts' comments to make it easier to comprehend and to match the most recent goods they provide. While the content may appear to be changed in certain places, Meta is not collecting, using, or sharing your data in new ways due to this policy modification. "We continue not to sell your information".

Internal privacy specialists from the legal, policy, and product teams assess the project's privacy concerns and determine whether any changes need to be made before launch to mitigate such risks. This evaluation is especially critical for protection, stability, and decency techniques, as they may involve the use of a wide range of data to detect and prevent potential issues. This data includes the content users publish, their connections with others, and the information they provide when using Meta's products and services, such as during the account registration process. Additionally, metadata, such as the geographic location of a photograph or the timestamp indicating when a file was created, as well as information about a users's device, network connection, device's operating system, I.P. address, connection speed, and interactions with individuals, accounts, hashtags, Facebook groups, and Pages to whom they are connected, are all examples of the types of information considered in this evaluation.

C. Privacy Centre

The GDPR of the E.U. and the California Consumer Privacy Act (CCPA) are two significant developments in privacy and data protection laws and regulations that seek to increase the transparency of data activities. To ensure that people understand privacy policies, businesses must communicate data practices and user rights and adapt policies to new technologies.

Earlier this year, Meta introduced the Privacy Center as a resource for users to gain insights into Meta's approach to privacy across its various applications and technologies. The Privacy Center, which provides direct access to the updated Privacy Policy, is now available to users of Facebook on desktop and mobile devices.

The Privacy Center is a one-stop shop for users' privacy concerns, where they can learn about how Meta uses Data, implement some of the different privacy options provided, and brush up on critical account security advice and tools. Meta will also keep adding guides and controls to it.

D. Updating Controls for User Privacy

New Audience Controls: Meta has included a new feature to let you manage who sees someone's Facebook posts. When someone sets a default audience, the audience option will apply to new Facebook posts they share on their timeline unless they choose a different audience for a specific post. Previously, a person's default audience for postings matched the most recently selected audience. So, if a person had just published a public post, all of the following postings would be public as well. This new setting will assist the users in ensuring that they are sharing with the appropriate individuals in the community.

New Methods for Managing the Ads We See: Meta has combined the Ad Themes and Interest Categories controls into a single control accessible on Facebook and Instagram, offering a broader range of ad topics. This feature allows users to set their preferences for ad topics through a single control. This control encompasses the interest targeting categories that marketers utilize to reach them and the content they encounter in advertisements (Anderson, 2017). Fig. 6 shows the timeline depicting the Facebook events from 2018 till recently.

E. Transparency and Control

Meta acknowledges that using a user's mobile number or national ID to regain account access may raise privacy concerns. Consequently, they consider it essential to grant users access to their submitted information. Users have the option to modify or remove the secure contact information they provide to Facebook through their Account Center. Additionally, individuals can exercise control over the retention of their identity cards by reviewing the ones they have submitted during a security check in the Account Center. According to their policy, Facebook retains ID information for a period of one year. This retention period is instrumental in enabling security teams to verify the authenticity of account holders and train algorithms to identify potential ID fraud and other related issues. Users who have shared their ID with Facebook can choose to opt out of training and request that their ID be retained for only 30 days to confirm their profile. It's important to note that Facebook requires an exact match between a profile or account and a government-issued identity, although this is not the sole criterion for determining legitimacy. Online, individuals have more flexibility to emphasize various aspects of their identities. For example, someone may want to create a Page for their business and engage with different audiences.

We also acknowledge that for a variety of reasons, many people, including transgender people, do not use the name indicated on their birth certificate or other legal papers. Moreover, approximately 1 billion people worldwide lack access to official identification documents. We are looking into alternative methods of identity verification that do not require government identification. However, given the constraints that currently exist and the legitimate concerns that some people may have about requests for identity information, it is even more critical that government identification requests made by Meta be specific and tailored (Davies, 2015). Furthermore, almost 1 billion individuals worldwide lack access to official identification documents.

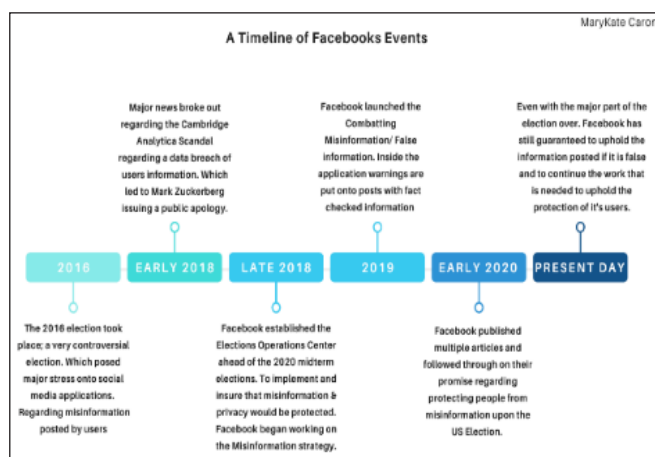


Fig. 6: Timeline of Facebook Events

F. Evolving Integrity - New Obstacles for the Metaverse

Every year, new environmental and technological developments pose challenges for Meta's products and services and their users. As new laws, market trends, and user expectations for privacy, safety, and functionality evolve, Facebook, Instagram, Messenger, and WhatsApp adapt. Meta believes that focusing its Integrity approach on users leads to an improved experience for the entire community. This necessitates staying at the forefront of change to understand the needs and desires of product users. The journey to the Metaverse is just beginning, with many products not expected to reach full realization for another five to ten years. Nevertheless, Meta is laying the foundation for ongoing discussions about how privacy, security, free speech, and civil rights can coexist in a virtual world that goes beyond a diverse and decentralized online experience offered by various companies. Meta recognizes its responsibility to act responsibly when developing technological advancements, clearly explain how data is used, and empower individuals to control what matters most to them. The goal is to minimize data collection, implement privacy strategies like differential privacy and on-device computation, and ensure transparency and user control in all products. Platform-level tools will be essential to help users manage their experiences and address unwanted content. Incorporating these features into first-party services is crucial, enabling other organizations to build their own solutions.

Additionally, Meta acknowledges that many of the safety and security issues observed on Facebook and Instagram may manifest differently in the Metaverse. For example, the design of virtual pets or creatures for sale in virtual reality may present unique challenges that do not align with real-world issues. Facebook and Instagram have policies prohibiting animal sales to mitigate animal suffering caused by backyard breeders or the exotic animal trade. In this regard, Meta recognizes the necessity of collaborating with experts from various fields, particularly in safety, to establish guidelines for the first-party augmented reality and virtual reality experiences that Meta may offer.

G. Twitter

According to Twitter's regulations, all information uploaded to the site is made public. However, users can alter this default behaviour to suit their preferences. According to Twitter's conditions, they gather private information such as a user's email address, phone

number, contacts in their address book, and public profile. According to the agreements, Twitter does not engage in the sale of user data to external entities. Nevertheless, the terms specify that Twitter may utilize personal data for delivering tailored advertisements and monitoring user activity on various apps, devices, and services across the internet. It's worth noting that users are not mandated to create an account before using the platform since most of the content is publicly accessible, although they are welcome to do so in order to fully access the services.

H. Concerns

The privacy evaluation procedure categorizes the policies of an application or service into the areas of concern by utilizing a subset of assessment questions designed to rapidly identify specific vendor policy practices. These concern areas, also shown in Fig. 7, comprise of assessment questions that help establish ratings for each individual concern.

Concern	Basic Score	Full Score
Data Collection: Protecting personal information	83	60
Data Sharing: Protecting data from third parties	100	85
Data Security: Protecting against unauthorized access	0	35
Data Rights: Controlling rights to data	63	85
Data Sold: Preventing sale of data	75	45
Data Safety: Promoting responsible use	67	35
Ads & Tracking: Prohibiting the exploitation of users' decision making process	43	50
Parental Consent: Protecting children's personal information	50	20
School Purpose: Following student data privacy laws	0	0
Individual Control: Controlling data use	NA	40

Fig. 7: Evaluation of Privacy Concerns

I. Security

As previously mentioned, tags and search engines can be used to locate a user's tweets on Twitter. When users visit a page with a "tweet" button, Twitter, similar to Facebook, has the ability to track their browsing history, including the date and time of their visits. This tracking is conducted by the network to provide recommendations. Twitter also utilizes targeted advertisements for the same purpose and maintains records of every application a

person has installed on their smartphone. Like Facebook, Twitter also tracks users' locations and phone connections (Twitter Privacy Policy, 2018). However, unlike Facebook, Twitter's public platform policy, rather than that of a social network, presents advertisements in a more reasonable manner. Additionally, the company simplifies the process for individuals to opt out of receiving customized emails and ads.

In an effort to make its policy language more user-friendly, Twitter has restructured its policy into three distinct sections: data collection, data usage, and data sharing. This policy has been expanded to cover various forms of media beyond tweets. Moreover, new terminology is employed to explain how content on Twitter is customized to provide users with advertisements. The company has updated its privacy page to assist users in navigating this information and understanding the data collected about them, how Twitter uses it, and how to control these choices.

Twitter, a social networking and microblogging website, enables users to post and respond to messages known as "tweets." To engage users and simplify the understanding of the platform's most intricate features, the internet giant has introduced a brand-new privacy policy video game created by the award-winning gaming studio Momo Pixel. The website for the browser game "Twitter Data Dash" cautions that navigating the Twitter-verse might be challenging if you are unfamiliar with it. Therefore, to help users better comprehend their privacy policy, the company has developed this game. In the game, players assume the role of a blue dog named Data or one of its companions as they progress through four levels, avoiding obstacles and collecting bones. When a user collects all five bones on a level, a pop-up window appears, explaining one of Twitter's privacy policies and inviting users to learn more if they wish. Each pop-up window also provides an opportunity to tweet about their game progress.

V. IMPLICATIONS

Complex Privacy Policies: The research reveals that privacy policies, especially on major web platforms like Google, Meta, and Twitter, tend to be overly complex. This complexity makes it difficult for the average user to comprehend the terms, potentially leading to unwitting data consent.

User-Friendly Information Gap: The study points out the lack of user-friendly information in these policies, hindering informed decisions about data privacy. Users may not fully grasp how their data is utilized and shared.

Regulatory Influence: The impact of privacy regulations, such as GDPR, on privacy policies is discussed. While GDPR has led to more readable policies, it also underscores the need for regulatory oversight.

Data Collection and Monetization: Leading web platforms amass extensive user data, often monetizing it through third-party sales. This raises concerns about user data protection and control.

Transparency and Control: Efforts by platforms like Meta and Twitter to enhance transparency and user control are highlighted. These initiatives reflect a growing recognition of user empowerment in data privacy.

User Awareness: The findings underscore the importance of users becoming more informed about data usage on web platforms. It emphasizes reading policies and understanding the implications of sharing personal information.

Future Research: The research suggests future investigations, including exploring privacy policies in the context of IoT and assessing the effectiveness of user education on data privacy.

VI. LIMITATIONS AND FUTURE RELEVANCE

Our research is representative of the privacy policies related to user data and how it is being used on various web platforms. Expanding the scope of the inquiry to encompass emerging threats, relevant data (such as the nature of personal data, processing methods, storage, security measures, and consent revocation), and various digital applications, especially in the realm of the Internet of Things (IoT), would be fascinating. It will require much work on the community and the regulators to fully convey all pertinent information while still keeping policies concise, easy to comprehend, and interesting enough for users to grasp what they consent to.

VII. CONCLUSION

Privacy has become a significant concern within the realm of online commerce platforms. The research conducted in this study represents the privacy policies related to user data and their utilization on various web platforms. This sheds light on the evolving landscape of data protection and user privacy in the digital age (Antón et al., 2002).

The scope of this investigation could be expanded to encompass new risks, relevant data (such as the type of personal data, data processing methods, storage, security measures, and consent revocation), and other digital applications, particularly within the Internet of Things domain. Achieving this will necessitate substantial efforts from both the community and regulatory bodies to effectively communicate all pertinent information. This should be done while ensuring that policies remain concise, easy to comprehend, and engaging for users, allowing them to understand what they consent to when sharing their content publicly for others to view, like, comment on, and retweet.

Furthermore, concerns regarding user privacy on the platform should be addressed, especially in light of allegations by a whistle-blower that the company misled authorities about inadequate security and spam issues. Users have the ability to control unintentional disclosures and regulate what information Twitter shares about them on the site, thereby preserving their privacy.

REFERENCES

- Anderson, B. (2017, February 13). The rise of the weaponized AI propaganda machine. *Scout: Science Fiction + Journalism*. Medium. Retrieved from <https://medium.com/join-scout/the-rise-of-the-weaponized-ai-propaganda-machine-86dac61668b>
- Caramujo, J., & Da Silva, A. R. (2015). Analyzing privacy policies based on a privacy-aware profile: The Facebook and LinkedIn case studies. *IEEE 17th Conference on Business Informatics (CBI)*, 1, 77–84. doi:<https://doi.org/10.1109/CBI.2015.44>
- Davies, H. (2015, December 11). Ted Cruz using firm that harvested data on millions of unwitting Facebook users. *The Guardian*. Retrieved from <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>
- Dutt, N. S. (2020). Building the next-gen cyber security operating model in a digital eco-system. *Telecom Business Review*, 13(1), 65-68. Retrieved from <http://publishingindia.com/TBR/65/building-the-next-gen-cyber-security-operating-model-in-a-digital-eco-system/10907/16252/>
- Anton, A. I., Earp, J. B., & Reese, A. (2002). Analyzing Website privacy requirements using a privacy goal taxonomy. *Proceedings IEEE Joint International Conference on Requirements Engineering*, 23-31. doi:<https://doi.org/10.1109/ICRE.2002.1048502>
- Gaber, M. A., D'Alessandro, D. M., & Johnson-West, J. (2002). Reading level of privacy policies on Internet health Web sites. *The Journal of Family Practice*, 51(7), 642-645. <https://pubmed.ncbi.nlm.nih.gov/12160504/>
- Jansson, A., & Christensen, M. (Eds.). (2014). Media, Surveillance and Identity: Social Perspectives (Digital Formations, Vol. 84). *Peter Lang Pub.* <https://www.peterlang.com/document/1051218>
- Lewis, S. D., Colvard, R. G., & Adams, C. N. (2008). A comparison of the readability of privacy statements of banks, credit counseling companies, and check cashing companies. *Journal of Organizational Culture, Communications and Conflict*, 12(2), 87-94. https://journals.kozminski.cems-j.com/index.php/pl_cemj/pdf/Dr%20Mausmi%20Goel.pdf
- 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. doi:<https://doi.org/10.1287/isre.1040.0032>
- Pandey, A. S., Dixit, N., & Sagar, M. (2020). Data protection framework for India. *Telecom Business Review*, 13(1), 36-46. Retrieved from <http://publishingindia.com/TBR/65/data-protection-framework-for-india/10907/16248/>
- Peslak, A., Kovalchick, L., & Conforti, M. (2020). A longitudinal study of Google privacy policies. *Journal of Information Systems Applied Research*, 13(2), 54-65. Retrieved from <http://jisar.org/2020-13/n2/JISARv13n2p54.html>
- Rewaria, S. (2021). Data privacy in social media platform: Issues and challenges. *SSRN Electronic Journal*. doi:<https://doi.org/10.2139/ssrn.3793386>
- Sipior, J. C., Ward, B. T., & Connolly, R. (2013). Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management*, 26(6), 661-678. doi:<https://doi.org/10.1108/JEIM-07-2013-0043/FULL/XML>
- Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1), 36-49. doi:<https://doi.org/10.1287/ISRE.13.1.36.97>
- Van Eecke, P., & Truyens, M. (2010). Privacy and social networks. *Computer Law & Security Review*, 26(5), 535-546. doi:<https://doi.org/10.1016/J.CLSR.2010.07.006>