The Turkish Online Journal of Design, Art, and Communication
E-ISSN: 2146-5193

DOI: 10.7456/tojdac

Research Article / Araştırma Makalesi

USER DATA AND DIGITAL PRIVACY: PRIVACY POLICIES OF SOCIAL MEDIA PLATFORMS

KULLANICI VERİLERİ VE DİJİTAL MAHREMİYET: SOSYAL MEDYA PLATFORMLARININ GİZLİLİK POLİTİKALARI

Mustafa BÖYÜK[1]

ORCID: M.B. 0000-0002-1010-9048

Corresponding author/Sorumlu yazar:
[1] Mustafa Böyük
Ankara Yıldırım Beyazıt University, Türkiye
E-mail/E-posta: mustafaboyuk@aybu.edu.tr

Received/Geliş tarihi: 17.10.2024

Benzerlik Oranı/Similarity Ratio: %6

Revision Requested/Revizyon talebi: 14.11.2024

Last revision received/ Reviewed by teslimi: 03.12.2024

Accepted/Kabul tarihi: 14.12.2024

Etik Kurul İzni/ Ethics Committee Permission: Çalışmada etik kurul onayı gerektiren bir unsur bulunmamaktadır. / There is no elemet in the study that requires ethics committee approval.

Citation/Atıf: Böyük, M. (2025). User Data And Digital Privacy: Privacy Policies Of Social Media Platforms. The Turkish Online Journal of Design Art and Communication, 15 (1), 225-239. https://doi.org/10.7456/tojdac.1569287

Abstract
This study examines the privacy policies and personal privacy violations of the five most widely used social media platforms globally: Facebook, Instagram, X (Twitter), YouTube, and TikTok. Adopting a qualitative approach, the research employs document analysis and case study methods. The study population comprises the privacy policies of these platforms, which have extensive global user bases, while the sample includes the most recent privacy policies and significant past privacy violations of Facebook, Instagram, X (Twitter), YouTube, and TikTok. The study analyzes how user data is collected, processed, and protected, evaluating the compliance of these platforms with legal regulations such as the GDPR and KVKK. Through case analyses of incidents like the Cambridge Analytica scandal and TikTok's violation involving children's data, the findings underscore the need for stronger security measures and user-friendly control mechanisms to safeguard user privacy. The study also highlights that complex privacy policies are not well understood by users, thereby hindering the provision of informed consent. The research acknowledges certain limitations, including the focus on only five platforms and the restriction of data collection to the period between January 2024 and October 2024. In conclusion, the study emphasizes that both platforms and users must take responsibility for ensuring data privacy and security. It recommends that platforms develop transparent and straightforward privacy policies, while users enhance their media literacy. Furthermore, the study calls for future research to evaluate the impact of emerging technologies, such as artificial intelligence, on privacy practices.

Keywords: Personal Data, Privacy, Digital Media, Social Media, Digital Privacy

Öz
Bu çalışma, dünya genelinde en çok kullanılan beş sosyal medya platformunun (Facebook, Instagram, X [Twitter], YouTube ve TikTok) gizlilik politikalarını ve kişisel gizlilik ihlallerini incelemektedir. Araştırma, nitel bir yaklaşım benimseyerek doküman analizi ve vaka incelemesi yöntemlerini kullanmıştır. Araştırmanın evreni, dünya genelinde geniş kullanıcı kitlesine sahip bu platformların gizlilik politikalarıdır; örneklemi ise Facebook, Instagram, X (Twitter), YouTube ve TikTok'un en güncel gizlilik politikaları ve geçmişte yaşadığı büyük gizlilik ihlalleridir. Çalışma, kullanıcı verilerinin nasıl toplandığını, işlendiğini ve korunduğunu analiz ederek bu platformların GDPR ve KVKK gibi yasal düzenlemelere uyumunu değerlendirmiştir. Cambridge Analytica skandalı ve TikTok'un çocuk verileri ihlali gibi örnekler üzerinden yapılan analizler, kullanıcı gizliliği konusunda daha güçlü güvenlik önlemleri ve kullanıcı dostu kontrol mekanizmalarına ihtiyaç olduğunu ortaya koymaktadır. Araştırma ayrıca, karmaşık gizlilik politikalarının kullanıcılar tarafından anlaşılmadığını ve bu nedenle bilinçli onamın sağlanamadığını vurgulamaktadır. Çalışma kapsamında, yalnızca beş platformun incelenmesi ve veri toplama sürecinin Ocak 2024 ile Ekim 2024 tarihleriyle sınırlı olması gibi sınırlılıklar bulunmaktadır. Sonuç olarak, kullanıcı gizliliği ve veri güvenliği konusunda hem platformların hem kullanıcıların sorumluluk alması gerektiği belirtilmiş; platformların şeffaf ve sade gizlilik politikaları geliştirmesi, kullanıcıların ise medya okuryazarlığını artırması önerilmiştir. Ayrıca, yapay zekâ gibi yeni teknolojilerin gizlilik uygulamaları üzerindeki etkilerini değerlendiren ileri araştırmalara ihtiyaç duyulduğu sonucuna varılmıştır.

Anahtar Kelimeler: Kişisel Veri, Mahremiyet, Dijital Medya, Sosyal Medya, Dijital Mahremiyet

INTRODUCTION

The rapid progress of digitalization has led to social media platforms becoming indispensable parts of daily life. Platforms such as Facebook, Instagram, X (Twitter), YouTube, and TikTok have radically changed the way individuals communicate, share information and interact (Statista, 2023). While these platforms allow users to create and share content and interact with other users, they also collect large amounts of data and use it for various purposes. However, with this transformation, the protection of privacy in the process of collecting, processing and sharing user data has become an important concern (Acquisti, Brandimarte, & Loewenstein, 2015).

Social media platforms are able to analyze user behavior through large datasets obtained from user interactions and use these data to provide targeted advertisements, personalize user experiences, and improve platform functionality (Tufekci, 2015). However, these data collection processes pose serious threats to user privacy and weaken user control over their personal data. Solove (2009) stated that the protection of privacy in the digital age is becoming increasingly complex, and users are not sufficiently informed about data collection processes. This situation makes it difficult for users to provide informed consent and can paves the way for privacy violations.

The main purpose of this study is to analyze the current state of the processing and protection of user data by examining the privacy policies and personal privacy violations of social media platforms in detail. The objectives of this study include understanding the data collection, processing, and sharing processes of social-media platforms, evaluating the effects of past privacy violations, and making recommendations to increase users' control over their data in this context. In this context, this study aims to answer the following research questions:

1. How are the privacy policies of Facebook, Instagram, X (Twitter), YouTube, and TikTok structured in terms of collecting, processing, and sharing user data?
2. What are the similarities and differences between the privacy policies of these platforms? Which practices stand out in terms of processing user data?
3. What types of personal privacy violations have been experienced on these platforms in the past and how have these violations affected user trust and the image of the platforms?
4. What measures have been taken and policy changes have been made by the platforms after privacy breaches?
5. To what extent do the privacy policies and data processing practices of these platforms comply with relevant legal regulations, such as the GDPR and KVKK?

The research adopted a document analysis approach, which is a qualitative method. The privacy policies, user agreements, press releases, and blog posts published on the official websites of the selected social media platforms were analyzed. In addition, news articles and academic studies on past privacy violations were also included in the study. The data obtained will be analyzed in detail using content and thematic analysis methods, and the similarities and differences between the data management practices of social media platforms will be revealed.

This research has some limitations. The privacy policies and data breaches of social media platforms are constantly being updated. Therefore, data obtained during the research process may not reflect future changes (Yin, 2018). This study analyzed the five most widely used social media platforms worldwide (We Are Social, 2024). Although a larger sample would enable a comparative analysis of different platforms, this study aimed to provide an in-depth analysis by focusing on key platforms (Dhagarra, Goswami, & Kumar, 2020). Moreover, the difficulty in obtaining detailed information about some privacy violations limited the full-scale data analysis.

This study aims to contribute to understanding the current state of social-media platforms’ data privacy policies and user privacy. The findings aim to contribute to the protection of user privacy by providing recommendations for the development of more transparent, ethical, and user-oriented policies in the social media ecosystem. In addition, this study will contribute to the academic literature and pave the way for further research into data management and privacy practices of social media platforms.

As a result, this study aims to contribute to the development of strategies to improve user data security by comprehensively addressing the current situation regarding the privacy policies of social media platforms and personal privacy violations. In the following sections of the study, detailed analyses will be presented under main headings, such as the literature review, methodology, findings, discussion, conclusion, and recommendations.

SOCIAL MEDIA AND USER DATA

With the rapid advancement of digitalization, social media platforms have become indispensable parts of daily life. These platforms have radically changed the way users communicate, share information, and interact. However, with this transformation, the protection of privacy in the process of collecting, processing, and sharing user data has become a major concern. This literature review comprehensively addresses the data privacy policies of social-media platforms, personal privacy violations, and legal regulations in this context.

Social media refers to digital platforms where users can create, share, and interact with each other, while data privacy refers to the protection of privacy in the processes of collecting, using, and sharing personal data (Regan, 2015). Social media platforms are able to analyze user behavior and use such data for various purposes due to the large datasets of user interactions (Kumar, Dixit, Javalgi, & Dass , 2016).

Social media platforms collect user data in various ways. These data cover a wide range of topics, such as shared content, likes, comments, clicks, and device information (Marwick & Boyd, 2014). These data are used to personalize user experiences, deliver targeted ads, and improve platform functionality (Mayer-Schönberger & Cukier, 2013). For example, Facebook and Instagram have analyzed user data to show ads that target user interests (Isaak & Hanna, 2018).

Some major privacy breaches in the past have exposed the inadequacy of social-media platforms' data management policies. For example, in 2018, Facebook's Cambridge Analytica scandal caused a major crisis when the data of 87 million users were used for political campaigns without authorization (Cadwalladr & Graham-Harrison, 2018). Such breaches have led to loss of user trust and the imposition of legal sanctions (Tufekci, Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency, 2015).

One of the most important legal regulations in the field of data privacy is the European Union's General Data Protection Regulation (GDPR), which imposes strict rules on the protection of user data and the transparency of data processing processes (European Union, 2016). In Türkiye, the Law on the Protection of Personal Data (KVKK) is the main legislation in this field. Social media platforms update their data processing policies and protect user data to comply with relevant legal regulations.

Users control over their data is recognized as a central element of data privacy policies. Acquisti, Taylor and Wagman (2016) stated that users are often not sufficiently informed about data collection processes and therefore find it difficult to give informed consent. Social media platforms try to improve this situation by providing users with various tools to manage and delete data (Tufekci, 2015). Platforms such as X (Twitter) increase user control by allowing users to customize their privacy settings and download their data (Twitter, 2023).

Algorithms and Privacy

The algorithms used by social media platforms personalize the user experience, they can also lead to privacy violations. Zuboff (2019) explained this situation with the concept of 'surveillance capitalism' and argues that user data are used as an economic value, and privacy is violated in this process. While algorithms deliver content based on user preferences, user behaviors must be monitored and analyzed in detail (Acquisti, Taylor, & Wagman, 2016). This makes it difficult to protect the privacy of users (Tufekci, 2015).

Social media platforms must develop various strategies to prevent data privacy violations. First, it is important that data collection processes are transparent and that users are adequately informed about such processes (Marwick & Boyd, 2014). Second, strong encryption methods should be employed, and data storage centers should be secured (Payton & Claypoole, 2023). It is also important to provide tools that allow users to have more control over their data and increase user awareness.

Ethical debates on data privacy cover the responsibilities of social media platforms and user rights. Zuboff (2019) argued that the economic value of user data pushes ethical boundaries and jeopardizes user privacy. Ethical data management should not only comply with legal regulations and include policies that respect user privacy (Floridi, 2018a). In this context, social media platforms must act in line with ethical principles and fulfill their commitments to protect user data (Floridi, 2018b).

Technological and social developments are constantly shaping data privacy policies. Technologies such as artificial intelligence and machine learning have made data analysis processes more efficient; however, they have also brought new privacy risks (Zuboff, 2019). Social media platforms follow these technological developments and develop innovative solutions to update their data privacy policies and protect user data.

The perception of data privacy is also influenced by cultural and social factors. The importance of privacy and the expectations regarding data privacy vary across cultures (Regan, 2015). Social media platforms are localizing and adapting their data privacy policies by taking these differences into account while addressing global user bases. This enables platforms to provide better service to their users while, allowing them to develop more flexible and inclusive policies on data privacy.

ANALYZING THE PRIVACY POLICIES OF SOCIAL-MEDIA PLATFORMS

Social media platforms have become the largest sources of user data in the digital age. Platforms such as Facebook, Instagram, X (Twitter), YouTube, and TikTok engage in large-scale data collection and processing to personalize user experiences, increase advertising revenue, and optimize content flow. These practices have fueled global debates about their impact on user privacy. Privacy is closely linked to transparency in the collection, processing, and sharing of personal information, as well as individuals' control over these processes (Solove, 2009).

This section examines the global concept of privacy and its applications on social media platforms, followed by a detailed evaluation of these platforms' privacy policies and compliance with regulations worldwide, including the United States and Türkiye. Additionally, case studies on privacy breaches will highlight the strengths and weaknesses of these platforms in terms of user privacy and security. Privacy refers to protecting individuals' control over the collection, processing, and sharing of their personal information (Westin, 1968). In the digital age, privacy has evolved to encompass the confidentiality and security of personal data. On social media platforms, data such as shared content, interactions, browsing habits, and geographical location are heavily utilized for commercial purposes (Zuboff, 2019).

These platforms typically use various techniques to collect user data:

- **Direct User Information:** Data provided by users during registration, such as names, email addresses, birthdates, and phone numbers.
- **Indirect Information:** Data on user interactions, messaging activity, search histories, content consumption patterns, and device details, used to personalize services.
- **Third-Party Integrations:** Platforms share data with third parties, such as ad networks and analytics services, to establish a more extensive data processing network (Cadwalladr & Graham-Harrison, 2018).

As of 2024, approximately 4.9 billion people use social media globally, making these platforms integral to daily life (We Are Social, 2024). However, their approach to privacy and implementation of privacy policies varies across countries.

The European Union has introduced the General Data Protection Regulation (GDPR), the most comprehensive framework for privacy and data processing. GDPR mandates that social media platforms obtain explicit and informed consent when collecting user data. It also grants users the right to understand how their data is processed and request its deletion when necessary. GDPR has set a global benchmark for shaping privacy policies on social media platforms. In contrast, privacy and data security practices are not uniformly implemented worldwide. For example, in countries like China, state surveillance is heavily focused on social media data, while in developing countries, inadequate legal frameworks pose significant threats to user data security (Nishnianidze , 2023).

In the United States, home to many major social media platforms and their global user bases, no comprehensive federal data protection law exists. Instead, regulations vary by state and sector. For instance, the California Consumer Privacy Act (CCPA) is one of the most comprehensive frameworks, granting users rights such as knowing what data is collected about them, restricting data sharing, and requesting data deletion (Schneier, 2016). However, these regulations lack nationwide consistency.

The Cambridge Analytica scandal in the United States raised widespread awareness about the misuse of user data and intensified calls for stricter regulations. This scandal, involving unauthorized use of user data in political campaigns, highlighted the urgent need for more transparent data processing policies on social media platforms. In Türkiye, with approximately 70 million social media users, the market for social media platforms is significant (We Are Social, 2024). Privacy regulations are shaped by the Personal Data Protection Law (KVKK), enacted in 2016. KVKK establishes standards for the collection, processing, and transfer of personal data, emphasizing the concept of explicit consent. Social media platforms operating in Türkiye are required to comply with KVKK. For example, Türkiye has mandated that platforms establish local representatives to enhance transparency in data processing and protect user rights. However, challenges remain. Users often struggle to understand privacy policies, which are often expressed in complex terms, undermining informed consent processes. Furthermore, discrepancies between global and local regulations create additional threats to data security for users in Türkiye.

Social media platforms have become the most important data sources in the digital age in terms of the way they collect, process, and share user data. Platforms such as Facebook, Instagram, X (Twitter), YouTube, and TikTok collect data on a large scale to personalize user experiences and increase advertising revenues. In this section, the privacy policies of platforms, their impact on user privacy, and their legal compliance are discussed in detail.

Facebook and Instagram

Facebook and its subsidiary Instagram take a comprehensive data collection and processing approach. Facebook’s privacy policy covers a wide range of data, such as user content, messaging history, location information, and device information. These data are used to personalize user experiences and deliver targeted ads (Facebook, 2024). Instagram follows a similar data collection strategy but focuses specifically on visual content and engagement data (Instagram, 2024).

These platforms are committed to obtaining user consent when sharing user data with third parties. However, the Cambridge Analytica scandal reveals that this commitment was breached and user data were used without consent (Cadwalladr & Graham-Harrison, 2018). This incident demonstrates that data sharing practices require transparency and user consent.

X (Twitter)

X (Twitter) has adopted a more transparent approach to collecting and processing user data. The platform collects data such as user tweets, direct messages, and interactions. These data are used to improve the platform’s functionality and provide content personalization (Twitter, 2023). X aims to increase users' control over their data by providing them with various tools to manage their data and customize their privacy settings (Fuchs, 2021).

YouTube

YouTube, which is a video sharing platform operated by Google, collects data such as user viewing habits, search histories, and device information. These data are used to optimize content recommendations and improve advertising targeting (YouTube, 2024). YouTube is committed to obtaining user consent when sharing user data with Google services and third-party partners (Kumar & Singh , 2022). This helps the platform ensure transparency in its data sharing practices.

TikTok

By monitoring user interactions and content creation behaviors, TikTok continuously improves its algorithms and offers user-specific content streams. TikTok's privacy policy covers data such as user-generated content, user interactions, and device information (TikTok, 2024).While such data collection practices enrich user experience, they raise concerns about data privacy (Zuboff, 2019).

METHODOLOGY

This study adopts a qualitative research approach to examine the privacy policies and personal data breaches of social media platforms such as Facebook, Instagram, X (formerly Twitter), YouTube, and TikTok. Document analysis and case study methods were employed to gain a comprehensive understanding of these platforms' data collection, processing, and sharing practices, as well as to evaluate the impact of past privacy breaches.

Research Questions

- How are the privacy policies of Facebook, Instagram, X (Twitter), YouTube, and TikTok structured in terms of data collection, processing, and sharing?
- What are the similarities and differences between these platforms' privacy policies, and what practices stand out in terms of data processing?
- What personal privacy breaches have occurred on these platforms in the past, and how have these incidents affected user trust and platform reputation?
- What measures were taken and policy changes implemented by the platforms following these breaches?
- To what extent do the privacy policies and data processing practices of these platforms comply with legal regulations such as the GDPR and KVKK?

These research questions were designed to define the study's focus and clarify the topics for analysis.

Research Framework

The study employs document analysis to investigate the privacy policies and personal data breaches of leading social media platforms, including Facebook, Instagram, X (Twitter), YouTube, and TikTok. Document analysis is a qualitative research method that systematically examines written materials in detail (Bowen, 2009). Documents analyzed include official privacy policies, user agreements, press releases, and blog posts from the platforms.

Content analysis was applied to the collected data to identify, extract, and interpret recurring themes, patterns, and meanings systematically (Krippendorff, 2018). This process enabled the identification of similarities and differences across platforms' policies on data collection, processing, sharing, and protection. Additionally, case study analysis was used to explore past privacy breaches in depth (Yin, 2018). This method facilitated a contextual evaluation of major incidents on each platform, assessing their impact on user trust and platform policies.

Sampling

A purposive sampling method was employed to select five major social media platforms (Facebook, Instagram, X (Twitter), YouTube, TikTok), based on their widespread global usage, large user bases, and significant past privacy breaches (We Are Social, 2024). The selection aimed to provide a comprehensive analysis of these platforms' global impact and practices regarding data privacy.

The sample included an analysis of the most recent privacy policies and major data breaches associated with each platform. Key cases examined included Facebook's 2018 Cambridge Analytica scandal, Instagram's 2019 data breach, Twitter's 2018 password security incident, YouTube's 2019 child data violation, and TikTok's 2020 privacy breach (Cadwalladr & Graham-Harrison, 2018; Fuchs, 2021).

Data Collection

Data were collected between January 2024 and October 2024. This process involved analyzing updated privacy policies, blog posts, press releases, and user agreements available on each platform's official website. Secondary data regarding past privacy breaches were also gathered.

Data Analysis Methods

The selected documents were systematically analyzed to examine the platforms' data collection, processing, sharing, and protection practices. This method provided an overarching framework for understanding the privacy policies of social media platforms. Data extracted from the documents were coded through content analysis to identify general trends, common themes, and significant differences in the policies (Krippendorff, 2018). Themes such as GDPR and KVKK compliance, the economic value of user data, and the effectiveness of user control mechanisms emerged during this process.

Significant privacy breaches (e.g., the Cambridge Analytica scandal, TikTok’s child data violations) were addressed using case study analysis. Each case was thoroughly examined within its context to evaluate the platforms' data protection practices and the impact of these incidents on user trust (Yin, 2018).

Limitations

This research has some limitations. Privacy policies and breaches are constantly being updated. Therefore, data obtained during the research process may not reflect future changes (Yin, 2018). Only five major social media platforms were analyzed in this study. Although a larger sample would enable a comparative analysis of different platforms, this study provided an in-depth analysis by focusing on key platforms. Furthermore, the difficulty in obtaining detailed information on some privacy breaches limited the full-scale data analysis.

The methodology section covers the methodological approach designed to provide a detailed analysis of the privacy policies and personal privacy violations of social media platforms such as Facebook, Instagram, X (Twitter), YouTube, and TikTok. The qualitative research methods, document analysis, and case studies enabled an in-depth analysis of the data management and privacy practices of these platforms. In this way, the efforts of social-media platforms to protect user data and the challenges faced in these efforts were comprehensively evaluated.

FINDINGS

Data Privacy on Social Media Platforms

As of 2024, the table below presents an overview of the data privacy policies of various social media platforms, including Facebook, Instagram, X (Twitter), YouTube, and TikTok. This table covers various aspects, such as data processing policies, user control, legal compliance, and data breach cases.

Table 1. Data Privacy Policies of Social Media Platforms.

Platform	Data Encryption Method	Data Storage Centers	Collected Personal Information	Collected Device Information	Data Sharing with Third Parties	Data Retention Period	User Control	Legal Compliance
Facebook	TLS 1.3	US, Europe	Shared content, messaging history, and financial information	OS, browser details, GPS, Wi-Fi, Bluetooth	Shared with business partners and developers	90 days	Users can download and delete data	GDPR, KVKK

Platform	Data Encryption Method	Data Storage Centers	Collected Personal Information	Collected Device Information	Data Sharing with Third Parties	Data Retention Period	User Control	Legal Compliance
Instagram	TLS 1.3	Same as Facebook	Same as Facebook	Same as Facebook	Same as Facebook	90 days	Users can freeze or delete their accounts	GDPR, KVKK
X (Twitter)	TLS 1.3	US, Europe	Shared content, messaging history, and tags	OS, browser details, battery level, GPS, Wi-Fi, Bluetooth	Shared for analysis and advertising	30 days	Users can download data	GDPR, KVKK
YouTube	TLS 1.3	Global	Search terms, video viewings, ad interactions	OS, browser details, WiFi, Bluetooth	Shared access to Google services and partners	60 days	Users can clear their watch history	GDPR, KVKK
TikTok	TLS 1.3	United States, Singapore, Ireland	User-generated content, interactions	OS, network type, device identifiers	Shared for analysis and advertising with partners	30 days	Users can delete accounts	GDPR, KVKK

By 2024, all platforms had adopted the TLS 1.3 encryption standard, which enhances data security during transmission and addresses vulnerabilities associated with older encryption algorithms (Rescorla, 2018). This development underscores the importance placed on data security by these platforms and their swift adoption of technological updates.

The geographical distribution of data storage centers is crucial to ensure data redundancy and comply with regional data protection laws. Platforms like Facebook and YouTube maintain extensive global data storage facilities, which means that their data are subject to various legal frameworks. This is especially important for ensuring compliance with regulations like GDPR (European Union, 2016).

Social media platforms collect various data, including shared content, messaging history, tags, and device information, to personalize user experiences and optimize advertising services. For instance, Facebook and Instagram are analyzing shared content and interactions to determine user interests (Facebook, 2024).

The sharing of data with third parties is a critical aspect of data privacy. Platforms generally share data with third-party partners for analysis, advertising, and service improvement. This sharing can have significant implications for user privacy, and it is crucial for users to be aware of such sharing. The Cambridge Analytica scandal demonstrated the serious consequences of improper data-sharing practices (Cadwalladr & Graham-Harrison, 2018).

User data control is a key component of privacy policies. Users have the option to freeze, delete, or download their data, thereby enhancing their control over their privacy. For example, Facebook allows users to download and delete their data, increasing users’ control over their personal information (Facebook, 2024).

All platforms comply with international and local data protection laws, such as the GDPR and KVKK, to ensure the protection of user data and privacy. However, data breaches remain a significant concern. Users must review these policies carefully and take the necessary precautions to protect their privacy.

Data processing policies vary based on users' media literacy, attitudes toward sharing data, and the adherence of states and commercial entities to security protocols. Therefore, it is important for users to be informed and thoroughly review privacy agreements.

Personal Privacy Violations on Social Media Platforms

The table below presents a comparative analysis of privacy violations on social media platforms such as Facebook, Instagram, X (formerly Twitter), YouTube, and TikTok. It examines platforms' past privacy violations, the consequences of such violations, the measures taken in response, and legal compliance.

Table 2. Privacy Violations on Social Media Platforms.

Platform	Past violations of privacy	Violation Consequences	Measures Taken	Legal Compliance	User Control
Facebook	Cambridge Analytica scandal (2018)	Data from 50 million users was misused; public backlash and legal inquiries	Stricter data sharing policies and improved user control tools	GDPR, KVKK compliance	Users can download and delete data
Instagram	Data leak (2019)	49 million users' personal data were leaked	Strengthen security protocols and two-factor authentication	GDPR, KVKK compliance	Users can freeze or delete their accounts
X (Twitter)	Data breach (2018)	330 million user passwords stored in plaintext	Updated encryption protocols, user notification	GDPR, KVKK compliance	Users can download data and customize their privacy settings
YouTube	Unauthorized collection of children's data (2019)	Fined $170 million by FTC; children's privacy violated	Revised data collection policies for children's content	COPPA, GDPR compliance	Users can clear their watch history
TikTok	Unauthorized collection of children's data (2019)	Fined $5.7 million by FTC; children's privacy violated	Stricter data collection policies for child users	COPPA, GDPR compliance	Users can delete their accounts

Facebook: Cambridge Analytica

The 2018 Cambridge Analytica scandal involving Facebook resulted in the unauthorized use of data from 50 million Facebook users for political campaigns. This incident is one of the most well-known examples of data privacy violations (Cadwalladr & Graham-Harrison, 2018).

The scandal sparked widespread public outrage over Facebook's data privacy policies and led to legal proceedings. The company was forced to take significant steps to restore user trust. This event highlighted the need for greater transparency and accountability in managing user data.

Facebook tightened its data-sharing policies and provided users with more tools to control their data. In addition, the company limited access to third-party applications to user information. These measures aim to increase user control over their data and prevent similar violations (Facebook, 2024).

Facebook also updated its policies to comply with data protection regulations, such as the GDPR and KVKK, which safeguard the privacy and protection of user data while regulating platforms' data processing practices (European Union, 2016; Resmi Gazete, 2016).
Users can download and delete their data, enhancing their control over their personal information. Such user control serves as a preventive measure against data privacy breaches (Facebook, 2024).

Instagram: Data leakage

In 2019, the personal information of 49 million Instagram users, including their email addresses and phone numbers, was leaked.

This incident led Instagram to review and strengthen its data security protocols. The exposure of personal information damages the platform's reliability and raises user privacy concerns. Security protocols were enhanced, and additional measures such as two-factor authentication, were implemented. These measures are intended to better protect user accounts and prevent future leaks (Instagram, 2024).

Instagram updated its policies to comply with legal regulations like GDPR and KVKK, to better protect user data (European Union, 2016; Resmi Gazete, 2016). Users can temporarily disable or delete their accounts, increasing their control over their personal data. Such control mechanisms help users safeguard their privacy (Instagram, 2024).

X (Twitter): Password Security Breach

In 2018, X (formerly Twitter) revealed that it had stored the passwords of 330 million users in plain text, indicating a significant security vulnerability (Twitter, 2018). Users were urged to change their passwords to secure their accounts. This incident prompted the platform to review and improve its security protocols.

The encryption protocols were updated, and users were informed. In addition, internal processes were reviewed to address security vulnerabilities. These measures aim to enhance user account protection (Twitter, 2023). X updated its policies to comply with data protection laws, such as the GDPR and KVKK, to assist the platform in better safeguarding user data (European Union, 2016; Resmi Gazete, 2016).

Users can download their data and customize their privacy settings to enhance their control over their personal information. Such control mechanisms help users protect their privacy (Twitter, 2023).

YouTube: Unauthorized Data Collection by Children

In 2019, YouTube was fined $170 million by the Federal Trade Commission (FTC) for collecting child data without consent (Federal Trade Commission, 2019b). Because of violations of children's privacy, YouTube was fined a substantial sum and had to review its policies. This incident made the platform more vigilant in managing the data of young users.

Data collection policies for children's content were revised, and stricter controls were implemented to better protect the data of young users (YouTube, 2024). YouTube updated its policies to comply with regulations such as COPPA and GDPR, assisting the platform in better safeguarding user data (Federal Trade Commission, 2019b; European Union, 2016).

Users can clear their watch history, which increases their control over their personal data. Such control mechanisms help users protect their privacy (YouTube, 2024).

TikTok: Unauthorized Data Collection by Children

In 2019, it was revealed that TikTok had collected children's data without consent, resulting in a $5.7 million fine by the Federal Trade Commission (Federal Trade Commission, 2019a). TikTok was fined for violating children's privacy and was forced to review its data collection policies. This incident prompted the platform to exercise greater caution when managing the data of young users.

Data collection policies for child users were tightened and stricter controls were implemented. These measures aim to better protect the data of young users (TikTok, 2024).

TikTok updated its policies to comply with regulations such as the COPPA and GDPR, assisting the platform in better safeguarding user data (Federal Trade Commission, 2019a; European Union, 2016).

Users can delete their accounts, which increases their control over their personal data. Such control mechanisms help users protect their privacy (TikTok, 2024).

This detailed analysis comprehensively addresses the privacy violations experienced by social-media platforms in the past, their consequences, and the measures taken. Users, considering this information, can gain a better understanding of platforms' data privacy policies and make informed decisions to ensure their own data security. The data processing policies of platforms vary according to users' media literacy levels, attitudes toward data submission, and adherence to the security protocols of states and commercial entities.

DISCUSSION: PRIVACY AND CONFIDENTIALITY VIOLATIONS IN SOCIAL MEDIA PLATFORMS

Social media platforms are at the center of the modern digital economy in terms of their collection, processing, and sharing of user data. Platforms such as Facebook, Instagram, X (Twitter), YouTube, and TikTok collect data on a large scale to personalize user experiences and increase advertising revenues. However, these processes raise serious concerns about user privacy.

Zuboff, Shoshana. 2019. "The Age of Surveillance Capitalism (2019) details how social media platforms use user data as an economic resource. Zuboff stated that these platforms monitor and analyze user behavior and sell these data to advertizers. This indicates a model of surveillance capitalism that violates user privacy. Facebook's Cambridge Analytica scandal is one of the most striking examples of this model. The scandal resulted in the unauthorized use of user data for political campaigns and led to a massive public outcry (Cadwalladr & Graham-Harrison, 2018).

The data collection practices of social-media platforms call into question the concepts of user consent and informed consent. Acquisti, Taylor, and Wagman (2016) stated that users are often not sufficiently informed about data collection processes and therefore cannot provide informed consent. Platforms such as Instagram and TikTok continuously improve their algorithms and offer user-specific content streams by monitoring user interactions and content creation behaviors. However, such data collection practices may violate user privacy and increase data security risks.

Privacy violations are important events that question the compliance of social media platforms with legal regulations. Data protection laws, such as GDPR and KVKK, regulate the data processing practices of platforms while ensuring the protection and privacy of user data (European Union, 2016; Resmi Gazete, 2016). However, these laws do not completely resolve ethical issues. Incidents of YouTube and TikTok collecting children's data without consent show that these platforms are struggling to comply with legal regulations (Federal Trade Commission, 2019a; Federal Trade Commission, 2019b). These violations have caused platforms to review their data collection policies and implement stricter controls.

Users' control over their personal data plays a critical role in protecting their privacy. Platforms such as X (Twitter) and Facebook offer users various tools to manage their data and customize their privacy settings. However, the effectiveness of such controls depends on how well users understand and use these tools. Tufekci (2017) stated that users often find it difficult to use such tools and thus cannot adequately protect their privacy.

The data processing policies of social media platforms also raise ethical issues. In an environment where the economic value of user data pushes ethical boundaries, platforms should pay more attention to the principles of transparency and accountability. Zuboff (2019) defined this situation as 'surveillance capitalism' and states that the economic value of user data pushes ethical boundaries. In the future, social media platforms are expected to develop more ethical and user-oriented data processing policies.

The privacy policies and violations of social media platforms exhibit a complex structure regarding the collection, processing, and sharing of user data. Users should carefully review these policies and take the necessary measures to protect the privacy of their data (Regan, 2015). The data processing policies of platforms vary according to users' media literacy levels, attitudes toward surrendering data and compliance with the security protocols of governments and commercial organizations. Therefore, users need to be aware of carefully scrutinize privacy agreements. The future development of more transparent, accountable, and user-oriented policies by social media platforms will be an important step toward protecting user privacy.

CONCLUSION

This study aimed to analyze the current state of social media platforms (Facebook, Instagram, X [Twitter], YouTube, and TikTok) privacy policies and personal privacy violations by examining how user data are processed and protected. The findings suggest that these platforms exhibit similar approaches to collecting, processing, and sharing user data, although there are differences in the nature of privacy violations and the responses to such breaches.

The privacy policies of the social-media platforms examined generally reflect efforts to provide transparency in the processes of data collection, processing, and sharing. However, the complexity of policies and the heavy use of legal terminology often hinder users from fully understanding them. Solove (2009) pointed out that the privacy policies of social-media platforms are often complex and difficult to comprehend. This lack of clarity prevents users from being sufficiently informed about data collection and processing practices. Specifically, Facebook and Instagram engage in extensive data collection and processing activities, analyzing user behaviors in great detail. In this context, platforms' ability to analyze user data poses a threat to user privacy.

The X (Twitter) platform also plays a significant role in analyzing user interactions and content preferences to deliver personalized content. However, some past privacy violations have revealed weaknesses in the platform's ability to protect user data. TikTok and YouTube also stand out by evaluating user interactions and content preferences algorithmically, offering highly personalized content.

Past privacy breaches have exposed platforms' inability to ensure data security and protect user privacy. The Cambridge Analytica scandal demonstrated the serious consequences of sharing user data without permission (Cadwalladr & Graham-Harrison, 2018). This incident severely damaged user trust and tarnished the platform's reputation. Such violations have significantly impacted user trust in these platforms and raised privacy concerns. Similarly, incidents of Instagram and TikTok collecting children's data without consent have shown that these platforms face challenges in complying with legal regulations. The X (Twitter) platform has also suffered from data breaches in the past, which have undermined user trust and damaged its reputation.

Regulations like the GDPR and KVKK regulate data processing activities on these platforms and protect user rights. Although the platforms examined in this study are striving to comply with these regulations, gaps remain in practice (Kumar & Singh , 2022). Acquisti, Taylor, and Wagman (2016) emphasize the need to improve user control over their data and enhance the processes of obtaining informed consent. Ethically, the practice of treating user data as an economic asset and using it for commercial purposes creates grounds for privacy violations (Zuboff, 2019).

The level of user control over their data plays a critical role in protecting user privacy. However, these findings demonstrate that users do not fully understand privacy policies and are unable to effectively utilize control mechanisms over their data (Tufekci, 2017). The difficulty users experience in comprehending the privacy policies of social-media platforms increases the likelihood of privacy violations. This situation highlights the need for platforms to make greater efforts to offer more transparent and user-friendly interfaces.
Recommendations for Platforms:

1. **Creating Transparent and Understandable Privacy Policies:** Platforms should revise their privacy policies using simple language to make them easier for users to understand (Solove,

2009). This method will help increase user awareness regarding data collection and processing practices.
2. **Developing User Control Mechanisms:** Platforms should offer more user-friendly interfaces and settings to enhance user control over their data. For example, simplifying processes such as data deletion, download, and adjustment of sharing permissions, is crucial.
3. **Strengthening Data Security Measures:** To prevent the recurrence of past privacy breaches, platforms must employ robust encryption methods and security protocols (Rescorla, 2018). Regular security audits and risk assessments should also be conducted.
4. **Adopting Ethical Data Processing Policies:** Platforms must use user data only for authorized purposes and should act in accordance with ethical principles (Zuboff, 2019). It is important not to share data with third parties without user consent.

This study examines privacy policies of social media platforms on a global scale, focusing particularly on examples from Europe and the United States. One limitation is the application of Turkish regulations, especially the impact of KVKK. It is believed that the privacy awareness of Turkish social media users may differ from that of users in Europe and the United States. Although KVKK contains parallels to GDPR, gaps in implementation hinder the full protection of user rights. Additionally, the lower levels of media literacy and the shortcomings in digital literacy among Turkish users pose challenges for understanding privacy policies, reflecting similar global issues.

This study provides a comprehensive examination of privacy policies and personal data breaches of social media platforms. However, further research focusing on Türkiye-specific regulations and user behaviors is crucial. Future studies should analyze the effects of Türkiye's legal frameworks on these platforms and explore ways to enhance user awareness and education on privacy rights.

Recommendations for Users:

1. **Increasing Media Literacy:** Users should read and attempt to understand privacy policies. By doing so, they can make informed decisions about how their data are processed and shared (Tufekci, 2017).
2. **Effectively Using Privacy Settings:** Users should use the privacy settings and control mechanisms offered by platforms and adjust the sharing permissions for their data.
3. **Security Measures:** Strong passwords should be used, and two-factor authentication methods should be activated (Rescorla, 2018).

Recommendations for Policymakers and Regulators:

1. **Updating and Enforcing Legal Regulations:** Regulations like the GDPR and KVKK should be updated considering technological advancements and emerging privacy risks and enforced effectively (Kumar & Singh , 2022).
2. **Strengthening Audits and Penalties:** Deterrent penalties should be imposed for privacy violations, and platforms should be regularly audited (Acquisti, Taylor, & Wagman, 2016).
3. **Raising Public Awareness:** Educational and information campaigns should be organized to raise public awareness of data privacy.

Recommendations for Academic Research and Future Studies:

1. **Conducting Further Research on Data Privacy:** More comprehensive and up-to-date research should be conducted on the privacy policies of social media platforms and user behaviors.
2. **Examining Cultural and Societal Factors:** Analyzing data privacy and user attitudes in different cultures is important for improving privacy policies.
3. **Monitoring Technological Developments:** The impact of technologies like artificial intelligence and machine learning, on data privacy should be studied, and the risks in these areas should be evaluated, with potential solutions proposed.

This study comprehensively addressed the current state of social-media platforms' privacy policies and personal privacy violations. The findings indicate that there are some shortcomings in the platform data processing practices, and user privacy is not fully protected. These results align with current academic studies and demonstrate the need to develop more transparent, ethical, and user-oriented policies in the social media ecosystem. In the future, it is anticipated that platforms' practices regarding data privacy will improve with the influence of technological developments and legal regulations. However, it is also crucial for users to remain informed and actively manage data control during this process.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature, 54*(2), 442-492.

American Psychological Association. (2020). *Publication Manual of the American Psychological Association (7th ed.).* APA.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27-40.

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* Retrieved from The Guardian: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of trust and privacy concerns on technology acceptance in healthcare: an Indian perspective. *International Journal of Medical Informatics*(141).

European Union. (2016). *General Data Protection Regulation (GDPR).* Official Journal of the European Union.

Facebook. (2024). *Facebook Privacy Policy*. Retrieved from Facebook: www.facebook.com/privacy/explanation

Federal Trade Commission. (2019a). *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law* . Retrieved from Federal Trade Commission: www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy

Federal Trade Commission. (2019b). *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*. Retrieved from Federal Trade Commission: https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law

Floridi, L. (2018a). *The Ethics of Information.* Oxford: Oxford University Press.

Floridi, L. (2018b). *The Logic of Information: A Theory of Philosophy as Conceptual Design.* Oxford: Oxford University Press.

Fuchs, C. (2021). *Social Media: A Critical Introduction.* London: SAGE Publications.

Instagram. (2024). *Instagram Data Policy*. Retrieved from Instagram: www.help.instagram.com/519522125107875

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica and Privacy Protection. Computer, 51(8), 56-59. *Computer, 51*(8), 56-59.

Krippendorff, K. (2018). *Content Analysis: An Introduction to Its Methodology.* London: SAGE Publications.

Kumar, N., & Singh , A. K. (2022). Impact of environmental factors on human semen quality and male fertility: a narrative review. *Environ Sci Eur, 34*(6).

Kumar, V., Dixit, A., Javalgi, R. G., & Dass , M. (2016). Research framework, strategies, and applications of intelligent agent technologies (IATs) in marketing. (44), 24-45.

Marwick, A. E., & Boyd, D. (2014). Networked Privacy: How Teenagers Negotiate Context in Social

Media. *New Media & Society, 16*(7), 1051–1067.

Mayer-Schönberger , V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think.* Boston: Houghton Mifflin Harcourt.

Nishnianidze , A. (2023). Surveillance in the Digital Age. *European Scientific Journal*, 24-80.

Payton, T., & Claypoole, T. (2023). *Privacy in the age of Big data: Recognizing threats, defending your rights, and protecting your family.* Maryland: Rowman & Littlefield.

Regan, P. M. (2015). *Legislating Privacy: Technology, Social Values, and Public Policy.* Chapel Hill: University of North Carolina Press.

Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3.* Retrieved from Internet Engineering Task Force: https://tools.ietf.org/html/rfc8446

Resmi Gazete. (2016). *Kişisel Verilerin Korunması Kanunu.* Retrieved from Resmi Gazete: www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf

Schneier, B. (2016). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* New York.

Solove, D. (2009). *Understanding Privacy.* Cambridge: Harvard University Press.

Statista. (2023). *Statista Research Department. Retrieved from h*. Retrieved from Number of social network users worldwide from 2010 to 2023.: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

The Economist. (2024). Ekonominin Trendleri. *Ekonominin Trendleri 2024.* The Economist Newspaper, New York.

TikTok. (2024). *Privacy Policy*. Retrieved from TikTok: https://www.tiktok.com/legal/privacy-policy-row?lang=tr-TR

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Law Journal*(13), 203-218.

Tufekci, Z. (2017). *Twitter and Tear Gas: The Power and Fragility of Networked Protest.* New Haven: Yale University Press.

Twitter. (2018). *Twitter Security Bulletin: Password Storage Vulnerability.* . Retrieved from Twitter: www.twitter.com/en/security-bulletin

Twitter. (2023). *Twitter Privacy Policy*. Retrieved from Twitter: https://twitter.com/en/privacy

We Are Social. (2024). *Digital 2024*. Retrieved from We Are Social: https://wearesocial.com/uk/blog/2024/01/digital-2024/

Westin, A. F. (1968). *Privacy and Freedom.* New York: Atheneum.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods (6th ed.).* Los Angeles: SAGE Publications.

YouTube. (2024). *YouTube Privacy Policy*. Retrieved from YouTube: https://www.youtube.com/intl/ALL_tr/howyoutubeworks/user-settings/privacy/

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: Public Affairs.