

Privacy and surveillance on social media: Awareness and tendencies of users in Türkiye

Ozkan Avcı*, Onur Sen** Mahmut Fevzi Cengiz***

*  Asst. Prof. Dr., Bartın Vocational School, Bartın University (drozkanavci@gmail.com)

**  Lecturer, Corresponding Author, Faculty of Communication, Ondokuz Mayıs University (onur.sen@omu.edu.tr)

***  Lecturer Dr., Eregli Kemal Akman Vocational School, Necmettin Erbakan University (mahmutfevzi@hotmail.com)

Abstract

The rapid spread of digitalization has made individuals' personal data more accessible which in turn makes privacy violations and surveillance processes more prominent. The main purpose of this paper is to assess social media users' privacy and surveillance awareness, their tendency to disclose personal information, and to discuss the effects of these processes at the individual and social level. A quantitative research design was employed. Data was collected from 800 participants through online and face-to-face surveys. Participants' social media usage habits and their attitudes toward privacy and confidentiality on social media were analyzed. The findings revealed that women have a higher awareness of surveillance and privacy violations, single individuals have a greater tendency toward privacy disclosure and privacy violation, and surveillance awareness decreases as the duration of social media usage increases. The results also indicate that participants have low awareness of surveillance and privacy violations and tend to disclose their personal information. This suggests that social media users should better understand potential privacy threats and implement higher caution and responsibility when sharing personal information.

Keywords: Digital Surveillance, Privacy and Data Security, Social Media Privacy, Privacy Perception, Self-Disclosure Behavior

Introduction

Social media use has become an integral part of the lives of billions of people. People use social media almost every day for one reason or another, such as communication with friends, networks, and societies, information exchange, and monitoring the lives of friends and loved ones. With the widespread use of social media, there are some risks involved, such as third-party unauthorized collection of personal data and violation of users' privacy and confidentiality.

As social beings, individuals consciously or unconsciously observe their surroundings. Surveillance takes place within social systems among friends and colleagues or is conducted by managers, companies, and governments (Brown, 2014, p. 1). Accordingly, the concept of oversight has traditionally referred to institutional mechanisms implemented by managers, governments, or corporations to exert control over individuals (Ball, 2010, p. 87). The growing presence of internet networks in daily life, particularly the

integration of social media into everyday routines, has introduced new forms of surveillance. In this context, social media surveillance refers to the monitoring and analysis of individuals' digital behaviors such as comments, likes, and shares on social media platforms (van der Schyff et al., 2020, pp. 1-2). Awareness of social media surveillance, on the other hand, refers to users' understanding of how social media companies collect, store, and use their personal data (van der Schyff & Flowerday, 2019, pp. 3-4).

Self-disclosure behavior on social media is a user's act of sharing personal information and messages with others on the platform (Brown, 2020, p. 2). Currently, social media platforms have become spaces where users share personal stories and disclose details about their daily and private lives (Miguel, 2016, p. 8). Social media platforms enable users to share personal information, including photos, videos, daily activities, emotions, opinions, and location, with others (Brown, 2020, p. 2). However, sharing intimate details of private lives with large and unknown audiences on social media entails various risks. The personal information and privacy of users who disclose extensive details about themselves may be compromised by third parties (Büchi et al., 2017, pp. 1272-1273).

With the rapid spread of digitalization, personal data has become more accessible through social media platforms. Consequently, this increased the visibility of privacy violations and surveillance processes. A literature survey revealed that Trottier (2011) examined surveillance on social media and Facebook's efforts to police its users; Nolan et al. (2011) investigated surveillance, autonomy, and privacy in children's social media use; Fuchs et al. (2013) analyzed internet surveillance in the context of Web 2.0 and the challenges of social media; Ghoshray (2013) studied employer privacy and surveillance in social media; Belapurkar (2018) studied information privacy concerns and surveillance in social media; Bolin and Jerslev (2018) analyzed surveillance and surveillance practices as represented in the media; Tagle et al. (2024) analyzed media surveillance in Argentina and Peru; Mannan (2025) explored the tension between surveillance practices and privacy rights; and Selvakumar (2025) examined factors affecting social media privacy.

The current study, on the other hand, aims to examine users' privacy perceptions, surveillance awareness, and privacy disclosure tendencies on social media platforms. The study also aims to investigate how these dimensions vary according to demographic characteristics (e.g., gender, marital status, age, education, income, and occupation) and usage patterns (e.g., daily usage time, platform preferences, privacy setting habits). The findings are expected to inform the evaluation of social media platforms' privacy policies and support the development of individuals' online privacy awareness.

The study sought answers to the following questions:

1. What is the impact of participants' demographic characteristics (gender, marital status, age, educational status, income, and occupation) on their privacy evaluations?
2. What is the impact of users' social media usage duration, purpose of use, and privacy setting habits on their privacy evaluations?
3. What is the relationship between privacy violations, surveillance awareness, and privacy disclosure tendencies among social media users?

Literature review

The rise of social media and the transformation of privacy

Traditionally, before social media, people used the Internet solely to consume content that is reading, watching, and purchasing products or services. However, individuals now actively engage in creating, exchanging, sharing, and discussing content through various platforms such as content-sharing sites, blogs, social networks, and wikis (Kietzmann et al., 2011, p. 241). Social media refers to a collection of digital platforms and applications that enable users to create and share content online, interact with content from others, and form communities. These platforms and apps facilitate interaction among individuals, companies, organizations, politicians, and governments with large audiences.

Social media represents internet-based platforms that enable users to interact opportunistically and selectively self-present, either in real-time or asynchronously, to both broad and narrow audiences who derive value from user-generated content and perceived social interaction (Carr & Hayes, 2015, p. 50). As of the start of the year 2025, it is estimated that of the world's 8.20 billion people, 5.78 billion are mobile phone users, 5.56 billion are internet users, and 5.24 billion are social media active users. On average, internet users spend 2 hours and 21 minutes on social media daily. Compared to previous years, people now rely on connected technology for a much broader range of activities. However, statistics on internet privacy indicate that fewer than 3 out of 10 adult internet users are concerned about what companies do with their personal data. These figures somehow indicate a decline from previous years in the percentage of adult internet users concerned about online privacy. In this regard, many users tend to select the "accept all" option for cookies on websites. However, in regions with regulations like the European Union's General Data Protection Regulation (GDPR), individuals display a little higher sensitivity to privacy concerns (We Are Social, 2025). The GDPR envisages certain obligations to protect the personal data of EU citizens throughout Europe, which include regulations on transferring personal data to non-EU countries and international organizations. The regulation defines personal data as "Personal data is any information that relates to an identified or identifiable living individual (data subject)" (GDPR, 2025). Accordingly, personal data encompasses any information that can be used to re-identify an individual, including direct identifiers such as name, address, email, and IP address. This personal data can lead to the identification of a specific person, as well as de-identified data that, when combined, enable identification. However, irreversibly anonymized data is not considered personal data (European Commission, 2025).

As the use of the internet and social media becomes more involved in our daily lives, concerns regarding the unauthorized application of users' personal data naturally emerge. As individuals participate in social media for various reasons—spanning communication, socialization, shopping, and information seeking—their activities online reveal a lot of personal data. Moreover, users' activities on social media platforms not only expose their personal data but also make their characteristics predictable. Technology giants and social media companies employ artificial intelligence and machine learning-based data collection and analysis methods to gather users' personal and behavioral data in social media environments for various purposes. Additionally, this data is often utilized without users' consent.

The problem regarding non-consensual use of personal data gained a global-scale attention during the 2016 U.S. presidential election. Between 2014 and 2016, Cambridge Analytica was alleged to have acquired the personal data of approximately 87 million Facebook users via various channels. While the company obtained

consent from only 300,000 users, the vast majority of the data was collected without users' permission (Brown, 2020, p. 1). There are allegations that the data obtained by Cambridge Analytica without users' consent made their socioeconomic and psychosocial status predictable- was used to influence target groups and persuade them to vote for Donald Trump in the digital campaigns of U.S. presidential election in 2016. Facebook apologized to its users and the public after the incident surfaced. However, Mark Zuckerberg, the CEO of Facebook, blamed Cambridge Analytica for the Cambridge Analytica fiasco, calling it a "breach of trust." Facebook was criticized by the US government for not taking proactive steps to safeguard users' personal information and privacy (US Senate, 2018). Even though Facebook itself was not found to be directly linked with Cambridge Analytica, the platform was blamed by many of its users for allowing an external entity to use their personal data without consent (Afriat et al., 2020, p. 116). Furthermore, the Cambridge Analytica scandal unveiled the degree to which unethical behaviors on social media networks have led to violations of individual privacy. Data collected without the express knowledge of users was utilized in evaluating their socioeconomic and psychosocial statuses, hence manipulating their political decision-making processes.

Users typically consciously or unconsciously share personal information to access services on social media applications. However, this practice often puts their privacy at risk. Consequently, the methods social media platforms use to collect and analyze data are reshaping individuals' perceptions of privacy and social interactions. These platforms primarily employ the following mechanisms to collect and analyze user data (Kuehn, 2013; Zuboff, 2015, pp. 78-80; Sapountzi & Psannis, 2018, pp. 910-911; van der Schyff & Flowerday, 2019, pp. 1-3, Rajendran & Smilan, 2025, p. 312):

- Cookies and Tracking Pixels: Used to track users' behavior on websites and collect data on their interactions.
- Data Mining: Personal profiles are generated by analyzing users' shared content, likes, and comments.
- Third-Party Integrations: Social media platforms share data with third-party applications to gather more comprehensive information about users.

The mechanism explained above facilitates the collection and use of personal data without users' awareness. Boyd & Crawford (2011, p. 2) described this process, stating: "Data is increasingly digital air: the oxygen we breathe and the carbon dioxide that we exhale". In this metaphor, data obtained from online environments is compared to oxygen, the essential element of daily life, while digital traces such as browsing histories, clicks, and likes are likened to the carbon dioxide released. One of the master themes around discussions about modern society is the erosion of the value of privacy in social networks. Initially, as one's private domain of life, privacy was the domain of the individual, but in the context of networks, it becomes an amalgam of the personal and the public spaces (Heikkilä & Kunelius, 2016, p. 1). His change of privacy carries many worries about the way people reveal themselves on the internet and social networks, with whom they talk, and which data they disclose.

Surveillance awareness and disclosure behaviors on social media

Currently, social media plays a huge role in the way people communicate, and it has become the most common way of sharing information and expressing one's self. Still, these platforms are as well bringing too

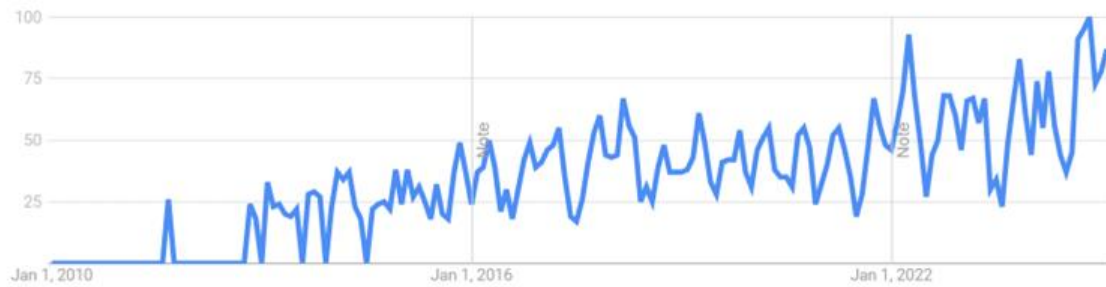
many privacy issues, such as the mass collection, analysis, and commercial use of people's personal data (Fuchs & Trottier, 2015, p. 114; Symeonidis et al., 2018, p. 206; van Schaik et al., 2018, p. 284). This is why surveillance awareness and individuals' self-disclosure behaviors on social media have become an important area of research at both individual and societal levels.

The concept of surveillance traditionally refers to institutional mechanisms implemented by governments or corporations to monitor and exert control over individuals (Wood & Webster, 2009, pp. 260-261; Ball, 2010, pp. 87-88, Lyon, 2017, p. 827). As the internet has permeated every aspect of daily life and social media use has become routine, new forms of surveillance have emerged within digital networks (Duffy & Chan, 2019, p. 4). As users spend more time online, a greater portion of their work and leisure activities becomes vulnerable to access, tracking, and analysis (Fuchs & Trottier, 2015, p. 130). The increasing popularity of social media enables individuals to voluntarily share their private lives, their thoughts in comments, and their interactions in posts, which is unlike traditional ways of surveillance, that is, the "surveillance state" or "surveillance society" (Lyon, 2017, p. 825).

Different surveillance technologies, such as data mining, machine learning, and artificial intelligence, are employed to monitor users on social media. Tech giants with billions of users—Google, Apple, Microsoft, Amazon, and Meta, collectively known as the "Big Five"—have become key players in these internet-based surveillance processes, tracking user data while also sharing it with state institutions (Lyon, 2017, p. 827). Not only the internet but also vast financial resources to be controlled through their managerial and economic by The Big Five. These companies are the one who have both, the giant money and the users data, which is close to trillions. Therefore, they have a very primary importance which nobody ever had or will have. With the user data they collect, they have the capability to predict and even shape human behavior. Zuboff (2015, p. 75) refers to this phenomenon as "surveillance capitalism." The primary objective of this new form of capitalism is to predict and modify human behavior to dominate the market and maximize profit (Zuboff, 2015, p. 76). In this process, users' posts, interactions, likes, comments, and other data are collected and analyzed through various algorithms and analytical tools. How much users actually understand these processes is a fundamental point to decide on their privacy.

In particular, users around the world have been more and more aware of social media surveillance since the 2010s. Figure 1 illustrates the Google search trend for the term "social media surveillance" between 2010 and 2025.

Figure 1: Google search trend for the term "social media surveillance" between 2010 and 2025



The results of the social media privacy research show that in most cases, clients are willing to trade in their privacy in return for low-level benefits (Aldehoff et al., 2019, p. 1185). Some of these studies suggest that users are often not aware that when they share their personal data, they are actually giving it to the creator or provider of the software or the app. Also, it's the fact, users just don't know about all the negative things may happen if they share their personal data. As a result, many users do not make a conscious or deliberate decision to disclose their personal information. Even users with a high level of awareness regarding the use of personal data may sometimes make mistakes due to the tendency to adopt new services and applications quickly, as well as the rapidly changing terms of use (Turow et al., 2015, pp. 3-5). People perceive online surveillance as an unavoidable consequence of the digital revolution. Even when they are aware of it, they feel compelled to accept it to avoid significant social or economic disadvantages. Only a small proportion of individuals actively seek to evade surveillance and adopt various strategies to do so (Degli-Esposti et al., 2017, pp. 77-78). Recent studies also show that privacy fatigue can drive protection disengagement, whereas higher literacy promotes precautionary behavior (Lyu et al., 2024). Moreover, qualitative evidence suggests that many users feel like 'captives' of digital media surveillance, which influences how they rationalize disclosure (Oguafor & Nevzat, 2025).

Self-disclosure is the act of "disclosing personal information to others" (Ma et al., 2016, p. 3857). On social media, self-disclosure refers to the behavior of users sharing information and messages about themselves with others. In a way, disclosure behaviors are the actions of people who like to share personal data and thoughts of other experiences on social media. Social media platforms give people to different types of information about each other such as biographical information, photos, videos, daily activities, emotions, opinions as well as location, online (Brown, 2020, p. 2). Sharing on social media websites can be considered as the telling of the person who you are, and it has now become the center of everyone's social life. However, not all users are equally inclined to share personal details about their lives. Studies indicate that individuals seeking to build more connections on social media tend to disclose more information compared to those who do not. Additionally, users are more willing to share personal information with distant acquaintances (Krasnova et al., 2010, pp. 122-123; Waters & Ackerman, 2011, pp. 112-113). Many social media users believe that their disclosure behaviors in online environments can help them build relationships, receive social support, and enhance their overall life satisfaction (Huang, 2016, p. 130). A large-scale experimental study further demonstrated that social norms strongly shape disclosure, reinforcing the privacy paradox (Masur et al., 2021).

Methodology

Scope and purpose of the study

The personal data shared on social media platforms poses risks which consequently cause privacy and confidentiality violations. Historically, privacy has been defined as a person's right to protect their own boundaries; however, the arrival of the digital era has changed this concept in social media settings and has also added new layers. Individuals navigate a balance between safeguarding their privacy and expressing themselves in digital environments. However, the data collection and analysis processes employed on social media platforms directly influence individuals' perception of privacy and their behavior on these platforms. This study aims to examine how users' privacy perceptions and disclosure behaviors are shaped on social media platforms. It also explores users' level of surveillance awareness on social media and its relationship with their privacy tendencies. The study tries to reveal individuals' privacy sensitivity in social media use and whether this sensitivity varies based on demographic characteristics such as age, gender, education level, and income level.

Design and sample

A quantitative study was designed to examine social media users' privacy perceptions, surveillance awareness, and disclosure tendencies. Similar studies in the field of privacy and surveillance on social media (e.g., Young & Quan-Haase, 2013; Kalaman, 2017; Büchi et al., 2017) have also adopted a survey-based quantitative research design to identify measurable differences between user groups. Research data were collected through online and face-to-face surveys with voluntary participation between 21 April 2024 and 20 June 2024, in Türkiye. The research data were analyzed using SPSS v.26. A significance level of $p < 0.05$ was adopted for the analyses. The simple random sampling method was employed to select participants. This method ensures that all individuals had an equal chance of selection, thereby minimizing bias (Neuman, 2014, p. 249). However, since age and education were later considered in sample composition, this procedure resembles elements of stratified sampling. To clarify, a sampling frame was generated from the pool of active social media users who could be reached via online survey invitations and local survey participation announcements. Within this frame, efforts were made to represent participants across age and education categories consistent with actual usage patterns.

Accordingly, the sample consisted of 800 participants most of whom were young and highly educated. This distribution aligns with the literature, which generally indicates a negative relationship between age and social media use and a positive relationship between educational level and social media use. Younger individuals tend to use social media more actively than older individuals, and interest in social media platforms increases with higher levels of education (Pew Research Center, 2024; We Are Social, 2025; Statista, 2025). Therefore, these variables were taken into account when determining the sample.

The change in participants' privacy perceptions was measured using the privacy scales developed by Kalaman (2017). However, scale questions specific to Facebook were adapted to refer to social media in general while maintaining the original wording. When adapting the questions, care was taken to ensure inclusivity. This was done while bearing in mind that social networking sites vary considerably in terms of the opportunities they offer and the privacy risks they pose. The questionnaire used in the study consists of four sections. The first section includes nine questions on the demographic characteristics and social media usage of the participants. The second section contains five questions on privacy violation, the third section

includes six questions on privacy disclosure tendency, and the fourth section comprises five questions on surveillance.

The Privacy Violation scale measures social media users' awareness about the privacy and security of their personal information. The scale items reflect users' perceptions of the ability of social media platforms to protect their personal information and how vulnerable they feel to security risks on these platforms. A high score on a sample item such as "I believe that social media platforms protect my personal data" indicates that the respondent is not aware of the risk of privacy violation or underestimates this risk. Consequently, the scale helps to determine users' level of awareness and vigilance about privacy violations. Higher scores indicate lower awareness of privacy violations.

The Privacy Disclosure scale measures the tendency of social media users to share their personal information. The items of the scale assess users' frequency and comfort in sharing their personal information (photos, videos, thoughts, location data, etc.) on social media platforms. A high score on a sample item such as "I share most of my personal data on social media platforms" suggests that the respondent was less concerned about privacy and more inclined to share personal information. Put simply, the scale helps to understand users' privacy boundaries and preferences for sharing information. Higher scores indicate a higher tendency to disclose personal information

The Surveillance scale measures social media users' awareness and concerns about the possibility of being monitored and surveilled in online settings. The scale items reflect users' thoughts on who can monitor them on social media platforms, how their personal information may be used, and how much control they have over these platforms. A high score on a sample item such as "I believe that no one can access my personal data on social media platforms unless I allow it" indicates that the respondent is not fully aware of the potential risks of privacy violations in online settings. The scale helps assess users' level of awareness and vigilance about privacy and security in online environments. Higher scores indicate lower awareness of surveillance.

Findings

Of the participants, 53.4% were female and 46.6% were male; 18% were married and 82% were single. 58.3% were 18-25 years old, 25.6% were 26-35 years old, 10% were 36-45 years old, and 7.1% were 46 years old or older. 60.8% were bachelor's degree graduates, 27.3% were associate degree graduates, 7.3% were high school graduates, and 4.6% were primary school graduates. In terms of socio-economic status, 45.1% had very low income, 43.8% had low income, 9.1% had medium income and 2% had high income. In terms of employment, 51.2% were students, 26% were workers, 10.4% were public servants, 4.1% were shopkeepers, 3.1% were retired, 2.3% were unemployed, 1.9% had other occupations, and 1% were homemakers (Table 1).

Table 1: Demographic characteristics of participants

Demographic Characteristics	Category	Frequency (n)	Percentage (%)
Gender	Female	427	53.4
	Male	373	46.6
Marital Status	Married	144	18.0
	Single	656	82.0
Age	18-25	466	58.3
	26-35	197	24.6
	36-45	80	10.0
	46 and above	57	7.1
Education	Primary School	37	4.6
	High School	58	7.3
	Associate Degree	218	27.3
	Bachelor's Degree	487	60.8
Income	Very Low	361	45.1
	Low	350	43.8
	Middle	73	9.1
	High	16	2.0
Occupation	Worker	208	26.0
	Public Servant	83	10.4
	Student	410	51.2
	Retired	25	3.1
	Unemployed	18	2.3
	Homemaker	8	1.0
	Shopkeeper	33	4.1
	Other	15	1.9
Daily Usage Time of Social Media	Less than 1 Hour	248	31.0
	2-3 Hours	284	35.5
	4-5 Hours	189	23.6
	6 Hours and Over	79	9.9
Primary Purpose of Using Social Media	Following Friends' Posts	163	20.4
	Keeping Up with Current Events and Finding Information	195	24.4
	Communicating	168	21.0
	Sharing Photos, Videos, etc.	174	21.8
	Other	100	12.4
	Yes	661	82.6

Configuring Privacy Settings on Social Media Platforms	No	139	17.4
---	----	-----	------

Regarding participants' daily social media usage, 35.5% spent 2–3 hours, 31% spent less than 1 hour, 23.6% 4–5 hours, and 9.9% 6 hours or more. Regarding the configuration of privacy settings on social media platforms, 82.6% of participants adjusted such settings, while 17.4% did not. Regarding the primary purpose of using social media, 24.4% used it for keeping up with current events and finding information, 20.4% for following friends' posts, 21.8% for sharing photos, videos, etc., 21% for communicating, and 12.4% for other purposes (Table 1). According to data published by We Are Social, at the beginning of 2025 -as in 2024- the biggest motivation for using the internet remains finding information, and more than 6 in 10 internet users' purpose is to stay connected with friends and family. Analysis of these data on social media usage revealed that the primary reason people use social media is to stay in touch with friends and family, followed by filling leisure time, and third, reading news to stay updated on current events (We Are Social, 2025). According to Statista (2025) data, internet and social media usage is higher for the 15-24 age group in all regions of the world, with an average daily time spent on social networks of 2-3 hours (151 minutes in 2023, 143 minutes in 2024). Consequently, it can be argued that the findings of this study are partially consistent with the participants' demographic characteristics.

Table 2: Item count and reliability coefficients of the privacy scales

Scale	Item Count	Reliability Coefficient
Privacy Violation	5	0.908
Privacy Disclosure	6	0.884
Surveillance	5	0.923

For Likert-type scales, it is essential to assess and report internal consistency reliability using Cronbach's alpha coefficient for each scale or subscale (Gliem & Gliem, 2003, p. 88). According to the results presented in Table 2, the scales exhibit high reliability.

Results

The analysis commenced with the calculation of descriptive statistics (means and standard deviations) for the privacy scale items, followed by an examination of the correlations between the scales, an assessment of normality, and a comparison of mean scores by demographic characteristics.

Table 3: Mean and standard deviation values of items in privacy scales

Scale	Privacy Items	Mean	SD	Overall Mean	SD	Corrected Item-Total Correlation
Privacy Violation	I think social media platforms enable me to communicate with my friends securely.	3.42	1.23	3.55	0.99	0.745
	I believe that if privacy settings on social media platforms are configured correctly and completely, personal data can be fully protected	3.51	1.08			0.784
	I confidently upload photos, videos, and texts on social media platforms because I know I will be protected.	3.66	1.14			0.749
	I do not consider social media a threat to my private life.	3.62	1.15			0.788
	I believe that social media platforms protect my personal data.	3.55	1.19			0.783
Privacy Disclosure	I share most of my personal data on social media platforms.	2.99	1.25	3.19	0.98	0.672
	On social media platforms, I sometimes share posts expressing compliments, love, affection, or reproach about my spouse, partner, relatives, or friends.	3.29	1.26			0.705
	On social media platforms, I sometimes meet new people and make friends.	3.03	1.28			0.633
	I sometimes have no hesitation in posting photos taken at the sea or pool on social media platforms.	3.17	1.20			0.651
	I sometimes post photos or videos taken at home on social media platforms.	3.30	1.20			0.775
	I share photos, videos, or posts about my important moments on social media platforms.	3.37	1.18			0.751
Surveillance	I believe that no one can access my personal data on social media platforms unless I allow it.	2.97	1.31	3.10	1.11	0.775
	I believe that when I configure privacy settings on social media platforms, no one except my friends can monitor me.	3.14	1.21			0.812
	I believe that as long as I do not engage in any illegal activities, I will not be monitored by the government through social media.	3.16	1.33			0.813

I believe that my information on social media platforms cannot be obtained and stored by the government and companies without my knowledge.	3.15	1.28			0.825
I believe that commercial companies cannot access my information on social media platforms without my permission.	3.12	1.24			0.775

SD: Standard Deviation

The inter-item correlation is expected to be >0.30 and the item-total correlation is expected to be >0.50 (Hajjar, 2018: 53). According to Table 3, item-total correlations ranged from a minimum of 0.633 to a maximum of 0.825. The item with the highest mean ($\bar{x}=3.66$) was "I confidently upload photos, videos, and texts on social media platforms because I know I will be protected" from the Privacy Violation scale, while the item with the lowest mean ($\bar{x}=2.97$) was "I believe that no one can access my personal data on social media platforms unless I allow It" from the Surveillance scale. The participants had the highest mean score on the Privacy Violation scale ($\bar{x}=3.55$) and the lowest mean score on the Surveillance scale ($\bar{x}=3.10$). These results suggest that participants are more likely to compromise their own privacy and have relatively higher awareness of surveillance compared to other measures.

Table 4: Correlations between the privacy scales

Scale		1	2	3
1- Privacy Violation	<i>r</i>	1.000	0.611	0.428
	<i>p</i>	-	0.000*	0.000*
2- Privacy Disclosure	<i>r</i>		1.000	0.549
	<i>p</i>		-	0.000*
3- Surveillance	<i>r</i>			1.000
	<i>p</i>			-

To identify correlations between the privacy scales, the Pearson correlation coefficients given in Table 4 were analyzed and correlations were evaluated at $p<0.05$ significance and 95% confidence level. In normally distributed data, Pearson correlation coefficients range between -1 and 1. A value of 0 indicates no linear or monotonic relationship, while values that approach the absolute value of 1 indicate stronger correlation (Schober et al., 2018, p. 1763). Correlation analysis revealed that the Privacy Violation scale showed a statistically significant positive relationship with the Privacy Disclosure ($r=0.611$, $p<0.05$) and Surveillance ($r=0.428$, $p<0.05$) scales. Additionally, a statistically significant positive correlation was observed between Privacy Disclosure and Surveillance ($r=0.549$, $p<0.05$) scales. According to the Pearson coefficients, the correlations between the scales are moderate.

Table 5: Normality analysis of the privacy scales

Scale	Skewness	Kurtosis
Privacy Violation	-0.631	-0.440
Privacy Disclosure	-0.354	-0.385
Surveillance	-0.245	-0.764

The normality of the data was examined before examining whether the participants' mean Privacy Violation scale scores differed according to their demographic characteristics. As seen in Table 4, The skewness and kurtosis values were close to zero, which means that the dataset had a normal distribution. Since the data were normally distributed, independent samples t-tests, and One Way Anova were performed (Tabachnick & Fidell, 2019, p. 68).

Table 6: Participants' mean scale scores by demographic characteristics

Variable		Privacy Violation		Privacy Disclosure		Surveillance	
		$\bar{X}$	SD	$\bar{X}$	SD	$\bar{X}$	SD
Gender	Female	3.48	1.01	3.13	0.98	2.99	1.15
	Male	3.63	0.96	3.26	0.97	3.23	1.06
	Test value	-2.172**		-1.885**		-3.092**	
	p	0.030*		0.060		0.002*	
Marital Status	Married	3.19	0.85	2.92	0.86	3.06	0.86
	Single	3.63	1.00	3.24	0.99	3.11	1.16
	Test value	-5.348**		-3.951**		-0.584**	
	p	0.000*		0.000*		0.560	
Age	18-25 (1)	3.69	1.05	3.19	1.01	3.03	1.22
	26-35 (2)	3.47	0.90	3.32	0.99	3.27	1.03
	36-45 (3)	3.24	0.82	3.15	0.86	3.16	0.80
	46 and above (4)	3.11	0.75	2.72	0.66	3.02	0.69
	Welch Test value	12.699***		9.956***		2.642***	
	p	0.000*		0.000*		0.050	
	Tamhane's T2 test	1>2, 1>3, 1>4, 2>4		1>4, 2>4, 3>4		-	
Education	Primary school (1)	2.78	1.17	2.72	1.13	2.78	1.20
	High school (2)	3.11	0.85	3.05	0.96	2.95	0.94
	Associate degree (3)	3.36	0.87	3.14	0.87	3.22	0.87
	Bachelor's degree (4)	3.74	0.98	3.26	1.00	3.09	1.22
	Welch Test value	19.350***		-		2.573***	
	Anova Test value	-		4.267***		-	

	p	0.000*		0.005*		0.057	
	Tamhane's T2 test	3>1, 4>1, 4>2, 4>3		-		-	
	Tukey	-		4>1		-	
Income	Very low (1)	3.41	1.05	3.13	0.98	3.14	1.07
	Low (2)	3.76	0.90	3.29	1.00	3.05	1.20
	Medium (3)	3.27	0.89	2.99	0.79	3.06	0.85
	High (4)	3.35	1.06	3.04	1.12	3.36	1.11
	Welch Test value	10.625***		3.238***		0.707***	
	p	0.000*		0.028*		0.551	
	Tamhane's T2 test	2>1, 2>3		2>3		-	
Occupation	Worker (1)	3.31	0.99	3.14	0.95	3.21	0.96
	Public Servant (2)	3.26	0.74	3.00	0.75	3.13	0.71
	Student (3)	3.81	1.00	3.31	1.05	3.05	1.30
	Retired (4)	3.03	0.69	2.72	0.67	2.97	0.60
	Unemployed (5)	3.38	0.80	3.00	0.76	3.20	0.77
	Homemaker (6)	2.77	0.90	2.72	0.72	3.02	0.82
	Shopkeeper (7)	3.30	0.73	3.09	0.83	3.15	0.85
	Other (8)	3.20	1.15	2.82	0.86	2.88	1.00
	Welch Test value	10.266***		3.857***		0.773***	
	p	0.000*		0.002*		0.612	
	Tamhane's T2 test	3>1, 3>2, 3>4, 3>7		3>4		-	
Daily Usage Time of Social Media	Less than 1 Hour (1)	3.23	1.15	2.98	1.17	3.00	1.16
	2-3 Hours (2)	3.75	0.83	3.34	0.83	3.09	1.10
	4-5 Hours (3)	3.69	0.86	3.15	0.88	3.09	1.15
	6 Hours and Over (4)	3.49	1.00	3.37	0.90	3.49	0.83
	Test value	12.541***		6.648***		6.164***	
	p	0.000*		0.000*		0.000*	
	Tamhane's T2 test	2>1, 3>1		2>1, 4>1		4>1, 4>2, 4>3	
Primary Purpose of Social Media Use	Following Friends' Posts (1)	3.32	0.97	3.10	0.90	3.11	1.01
	Keeping Up with Current Events and Finding Information (2)	3.61	0.89	3.22	0.89	3.12	1.04
	Communicating (3)	3.68	1.03	3.29	1.10	3.18	1.20
	Sharing Photos, Videos, etc. (4)	3.66	1.00	3.28	0.99	3.14	1.15

	Other (5)	3.38	1.07	2.92	1.00	2.84	1.17
	Welch Test value	-		2.882***		10.006***	
	Anova Test value	4.505***		-		-	
	p	0.001*		0.023*		0.188	
	Tamhane's T2 test	-		4>5		-	
	Tukey	4>1, 3>1, 2>1		-		-	
Configuring Privacy Settings on Social Media Platforms	Yes	3.56	0.99	3.18	1.00	3.11	1.13
	No	3.49	1.00	3.22	0.86	3.06	1.03
	Test value	0.772**		-0.554**		0.497**	
	p	0.440		0.580		0.619	

* $p < 0.05$, **Independent samples t-test, ***One-way analysis of variance, SD: Standard Deviation

As presented in Table 6, the significance of differences in mean scale scores based on participants' demographic characteristics was examined using a two-independent sample t-test for variables with two subgroups and a one-way ANOVA for variables with more than two subgroups. The equality of group variances was assessed using Levene's test. The corresponding p-value was given in the table based on whether the variances were equal or unequal. Accordingly, for homogeneous variances in the one-way ANOVA test, the Tukey test was applied using the ANOVA F-distribution, whereas when for heterogeneous variances, Tamhane's T2 test was applied based on Welch's correction.

According to the results given in Table 6, the Privacy Violation and Surveillance scale scores showed a significant gender-based difference that favors male participants. Additionally, single participants have significantly higher mean scores on the Privacy Violation and Privacy Disclosure scales. Regarding the Privacy Violation, participants in the 18–25 age group had a higher mean score than those in other age groups, while those in the 26–35 age group had a higher mean score than participants aged 46 and above. On the Privacy Disclosure scale, participants aged 46 and above had a lower mean score than those in other age groups. This is consistent with recent findings (Khan et al., 2023) that digital youth often normalize surveillance and continue to share information despite their awareness of risks.

On the Privacy Violation scale, participants with bachelor's degrees had a higher mean score than those with primary, high school, or associate degrees; additionally, participants with associate degrees had significantly higher mean scores than those with only primary education. On the Privacy Disclosure scale, participants with bachelor's degrees had a higher mean score than those with a primary education. Participants with low income showed higher privacy violation tendencies than those with very low- or medium-income levels. Furthermore, participants with low-income levels exhibited greater privacy disclosure tendencies than those with medium-income levels. In terms of occupation, students displayed higher privacy violations than workers, public servants, retirees, and shopkeepers. Students were also more likely to disclose personal information than retirees. This result may be related to the fact that retirees are significantly more likely to be concerned about online data security than younger individuals (We Are Social, 2025). In addition, this finding suggests that media patterns differ from those of older adults as a result of the extensive development of digital media communication technologies accompanied by the determined approach of digital youth to use them (Dunas et al., 2023, p. 26).

Regarding daily social media usage, participants who used social media for 2-3 hours and 4-5 hours daily exhibited higher privacy violations compared to those who used it for less than 1 hour. Additionally, participants who used social media for 2-3 hours or those 6 hours or more had higher mean Privacy Disclosure scores than those who used it for less than 1 hour. Furthermore, participants who used 6 hours or more displayed lower surveillance awareness than other users. Participants whose main purpose for using social media was to keep up with current events and finding information, to communicate or to share photos, videos, and similar content had a higher privacy violation mean scores than those who primarily used social media to follow their friends' posts. Moreover, participants who used social media to share photos, video, and similar content had higher mean scores on privacy disclosure than those who used it for other purposes. Finally, no significant differences were identified in participants' scale scores based on whether they configured privacy settings on social media platforms.

Discussion and Conclusion

Social media has become a platform that allows individuals to construct their identities in the online world, convey messages, and socialize. However, these virtual spaces change people's understanding of privacy, shape their consciousness of the importance of privacy issues, and reshape their behaviors in sharing information. The literature survey reveals that the concepts of privacy and confidentiality on social media platforms are shaped by individuals' awareness levels, platforms' data collection policies, and digital surveillance mechanisms implemented by governments (van der Schyff & Flowerday, 2019, pp. 3-4; van der Schyff et al., 2020, pp. 1-2).

What Mark Zuckerberg means by "Privacy is no longer a social norm" is that in today's digital age, the desire to protect privacy is not as prevalent or valued as it once was (Blank et al., 2014). The findings of this study directly address the main objective and research questions presented earlier. In line with the first research question, gender, marital status, age, education, and income significantly influenced privacy perceptions, disclosure behaviors, and surveillance awareness. For example, female participants displayed higher surveillance awareness, while younger and more educated participants were more prone to disclosure and violation behaviors. This demonstrates that demographic variables remain central to explaining differences in online privacy practices. Regarding the second research question, social media usage patterns also played a critical role. Longer usage time correlated with higher privacy violations and lower surveillance awareness, while platform purposes (e.g., information-seeking vs. sharing photos) shaped the type of privacy risks encountered. These findings highlight that not only who users are (demographics) but also how they use social media strongly affects their privacy outcomes. In relation to the third research question, the correlation analysis confirmed significant positive relationships among privacy violation, privacy disclosure, and surveillance awareness. This suggests that users who disclose more personal data are also more likely to perceive and even experience privacy violations, which paradoxically coexist with their relatively higher surveillance awareness. This aligns with the concept of the "privacy paradox" widely discussed in the literature (Young & Quan-Haase, 2013; Gerber et al., 2018).

The findings of the current study are consistent with the relevant literature. For instance, in Kalaman's (2017) study, which used the same scale questions for Facebook users, participants had low awareness regarding being surveilled and privacy violations, whereas their tendency to disclose personal information

was high. Büchi et al. (2017, p. 1272) found that individuals who use the internet more frequently exhibit more privacy problems. Additionally, Krasnova et al. (2010, p. 109) reported that users are more prone to privacy disclosure, primarily due to the ease of maintaining and developing relationships, as well as the enjoyment of social media platforms. This was also emphasized by Turow et al. (2015). They discovered that users have become less sensitive to protecting their privacy over time. Conversely, although a sizable portion of their sample had activated privacy settings on social media platforms, this did not result in any substantial increase in surveillance and privacy awareness. Young and Quan-Haase (2013) explained the privacy paradox that people are willing to disclose personal data on social networking sites despite expressing high levels of concern. While this indicates that the privacy of personal data is an important issue for online users worldwide, most users rarely put effort to actively protect their data and often disclose it voluntarily (Gerber et al., 2018).

The fact that younger and more educated individuals disclose more despite higher awareness suggests that educational interventions alone may not suffice; instead, platform-level transparency and stricter data protection regulations may be required.

Moreover, as prolonged use reduces surveillance awareness, strategies that continuously remind users of privacy risks (e.g., periodic notifications, visual warnings) could be implemented by platforms. The positive link between disclosure and perceived violations also underlines the need for digital literacy programs that emphasize the long-term consequences of voluntary self-disclosure. Comparative evidence shows that sustained media awareness campaigns (e.g., around TikTok) increase privacy concerns and risk perceptions, highlighting the importance of user-friendly governance and clearer platform policies (Choi & Thompson, 2025).

In conclusion, this study examined the relationship between social media and privacy from a multidimensional perspective and revealed the awareness and tendencies of social media users in Türkiye regarding privacy and surveillance. The results highlighted that the participants demonstrated inadequate knowledge of the safety and confidentiality procedures on personal information obtained via web-based social networking sites. In addition, the low awareness that increases the likelihood of individuals sharing their private information indicates that online sites should take more responsibility for ensuring the safety and confidentiality of their users. In this regard, it is important for social media platforms to develop more effective and transparent strategies for user training and enable users to manage their privacy more knowledgeably. In addition, increasing individuals' awareness of privacy protection and their understanding of disclosure behaviors is essential. The study's most significant contribution to the literature is to present the consequences of the social media habits people practice alongside demographic variables which disclose the level of protection individuals feel about privacy. Accordingly, a new perspective for research and practices in this field was also introduced. Future research should not only focus on privacy awareness levels but also investigate behavioral interventions that can reduce risky disclosure habits. Moreover, policymakers should explore how to make social media platforms' privacy policies more user-friendly and enforceable. Protecting privacy and defending individuals' digital rights are critical for the sustainability of social media use.

Bibliographical references

- Afriat, H., Dvir-Gvirsman, S., Tsurie, K., & Ivan, L. (2020). "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal. *The Information Society*, 37(2), 115-127. <https://doi.org/10.1080/01972243.2020.1870596>
- Aldehoff, L., Dankenbring, M., & Reuter, C. (2019). Renouncing privacy in crisis management? People's view on social media monitoring and surveillance. *ISCRAM*, 1184-1197, *Universitat Politecnica de Valencia*.
- Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, 51(1), 87-106. <https://doi.org/10.1080/00236561003654776>
- Belapurkar, R. (2018). Information privacy concerns and surveillance in social media. *International Journal of Law Management & Humanities*, 1(5), 186-194. <http://doi.org/10.1732/IJLMH.25140>
- Blank, G., Bolsover, G., & Dubois, E. (2014). A new privacy paradox: Young people and privacy on social network sites. In *Prepared for the Annual Meeting of the American Sociological Association*, (17), 1-33. <https://dx.doi.org/10.2139/ssrn.2479938>
- Bolin, G., & Jerslev, A. (2018). Surveillance through media, by media, in media. *Northern Lights*, 16(1), 3-21. https://doi.org/10.1386/nl.16.1.3_2
- Boyd, D., & Crawford, K. (2011). Six provocations for big data. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, September 2011, <http://dx.doi.org/10.2139/ssrn.1926431>
- Brown, A. J. (2020). Should I stay or should I leave?: Exploring (dis)continued Facebook use after the Cambridge Analytica scandal. *Social Media + Society*, 6(1), 1-7. <https://doi.org/10.1177/2056305120913884>
- Brown, I. (2014). Social media surveillance. In *The International Encyclopedia of Digital Communication and Society*, P.H. Ang and R. Mansell (Eds.), 1-7. <https://doi.org/10.1002/9781118767771.wbiedcs122>
- Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of internet skills for online privacy protection. *Information, Communication & Society*, 20(8), 1261-1278. <https://doi.org/10.1080/1369118x.2016.1229001>
- Carr, C. T., & Hayes, R. A. (2015). Social media: Defining, developing, and divining. *Atlantic Journal of Communication*, 23(1), 46-65. <https://doi.org/10.1080/15456870.2015.972282>
- Choi, S., & Thompson, L. (2025). Exploring the impact of media awareness on privacy concerns among social media users: A case study of TikTok. *Journal of Applied Security Research*, 1-26. <https://doi.org/10.1080/19361610.2025.2547204>
- Degli-Esposti, S., Pavone, V., & Santiago Gómez, E. (2017). Aligning security and privacy - The case of deep packet inspection. In M. Friedewald, J. P. Burgess, J. Čas, R. Bellanova & W. Peissl (Eds.), *Surveillance, Privacy and Security: Citizens' Perspectives*, 71-80, London, UK.
- Duffy, B. E., & Chan, N. K. (2019). You never really know who's looking: Imagined surveillance across social media platforms. *New Media & Society*, 21(1), 119-138. <https://doi.org/10.1177/1461444818791318>
- Dunas, D., Babyna, D., Salikhova, E., & Gladkova, A. (2023). 'Digital youth' agenda in social media: The study of popular Russian platforms. *World of Media. Journal of Russian Media and Journalism Studies*, 3, 26-40. <http://doi.org/10.30547/worldofmedia.3.2023.2>

- European Commission (2025). *Data protection explained*. Retrived from https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en
- Fuchs, C., & Trottier, D. (2015). Towards a theoretical model of social media surveillance in contemporary society. *Communications*, 40(1), 113–135. <https://doi.org/10.1515/commun-2014-0029>
- Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (Eds.). (2013). *Internet and surveillance: The challenges of Web 2.0 and social media*. Routledge Taylor & Francis Group.
- GDPR. (2025). *What is GDPR*. Retrived from <https://gdpr.eu/what-is-gdpr/>
- Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, 226-261. <https://doi.org/10.1016/j.cose.2018.04.002>
- Ghoshray, S. (2013). Employer surveillance versus employee privacy: The new reality of social media and workplace privacy. *Northern Kentucky Law Review*, 40(3), 593-626.
- Gliem, J. A., & Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. In *Midwest research-to-practice conference in adult, continuing, and community education*, (1), 82-87.
- Hajjar, S. T. (2018). Statistical analysis: Internal-consistency reliability and construct validity. *International Journal of Quantitative and Qualitative Research Methods*, 6(1), 46-57.
- Heikkilä, H., & Kunelius, R. (2016). Surveillance and the structural transformation of privacy. *Digital Journalism*, 5(3), 262-276. <https://doi.org/10.1080/21670811.2016.1256226>
- Huang, H. (2016). Examining the beneficial effects of individual's self-disclosure on the social network site. *Computers in Human Behavior*, 57, 122-132. <https://doi.org/10.1016/j.chb.2015.12.030>
- Kalaman, S. (2017). New media and transformation of privacy: Facebook cases in Turkey. *International Peer-Reviewed Journal of Communication and Humanities Research*, (14), 1-31.
- Khan, N. F., Ikram, N., Murtaza, H., & Asadi, M. A. (2023). Social media users and cybersecurity awareness: Predicting self-disclosure using a hybrid artificial intelligence approach. *Kybernetes*, 52(1), 401–421. <https://doi.org/10.1108/K-05-2021-0377>
- Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, 54(3), 241-251. <https://doi.org/10.1016/j.bushor.2011.01.005>
- Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25(2), 109-125. <https://doi.org/10.1057/jit.2010.6>
- Kuehn, A. (2013). Cookies versus clams: Clashing tracking technologies and online privacy. *Info*, 15(6), 19-31. <https://doi.org/10.1108/info-04-2013-0013>
- Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, 11, 824-842.

- Lyu, T., Guo, Y., & Chen, H. (2024). Understanding the privacy protection disengagement behaviour of contactless digital service users: The roles of privacy fatigue and privacy literacy. *Behaviour & Information Technology*, 43(10), 2007–2023. <https://doi.org/10.1080/0144929X.2023.2237603>
- Ma, X., Hancock, J., & Naaman, M. (2016). Anonymity, intimacy and self-disclosure in social media. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 3857–3869, <https://doi.org/10.1145/2858036.2858414>
- Mannan, M. A. (2025). Surveillance and privacy: Examining the complex interplay between national security and individual freedoms. In *Analyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions* (pp. 465–486). IGI Global Scientific Publishing.
- Masur, P. K., DiFranzo, D., & Bazarova, N. N. (2021). Behavioral contagion on social media: Effects of social norms, design interventions, and critical media literacy on self-disclosure. *PLoS ONE*, 16(7), e0254670. <https://doi.org/10.1371/journal.pone.0254670>
- Miguel, C. (2016). Visual intimacy on social media: From selfies to the co-construction of intimacies through shared pictures. *Social Media + Society*, 2(2), 1–10. <https://doi.org/10.1177/2056305116641705>
- Neuman, W. L. (2014). *Social research methods, qualitative and quantitative approaches* (Translated from the Turkish: S. Özge). Ankara: Siyasal Kitabevi.
- Nolan, J., Raynes-Goldie, K., & McBride, M. (2011). The stranger danger: Exploring surveillance, autonomy, and privacy in children's use of social media. *Canadian Children*, 36(2), 24–32.
- Oguafor, I. V., & Nevzat, R. (2025). "We are captives to digital media surveillance" Netizens awareness and perception of social media surveillance. *Information Development*, 41(2), 465–478. <https://doi.org/10.1177/02666669231171641>
- Pew Research Center (2024). *Social media fact sheet*. Retrived from <https://www.pewresearch.org/internet/fact-sheet/social-media/>
- Rajendran, Y. K., & Smilan, A. J. (2025). Data privacy and security risks in third-party app integrations. In *Analyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions*, D. Darwish & K. Charan (Eds.), 311–334. IGI Global. <https://doi.org/10.4018/979-8-3693-9491-5.ch014>
- Sapountzi, A., & Psannis, K. E. (2018). Social networking data analysis tools & challenges. *Future Generation Computer Systems*, 86, 893–913. <https://doi.org/10.1016/j.future.2016.10.019>
- Schober, P., Boer, C., & Schwarte, L. A. (2018). Correlation coefficients: appropriate use and interpretation. *Anesthesia & Analgesia*, 126(5), 1763–1768. <https://doi.org/10.1213/ANE.0000000000002864>
- Selvakumar, P. (2025). Factors influencing social media privacy. In *Analyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions* (pp. 15–38). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-9491-5.ch002>
- Statista (2025). *Trending facts & insights*. Retrived from <https://www.statista.com/markets/424/internet/>
- Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J., & Preneel, B. (2018). Collateral damage of Facebook third-party applications: A comprehensive study. *Computers and Security*, 77, 179–208. <https://doi.org/10.1016/j.cose.2018.03.015>

- Tabachnick, B. G., & Fidell, L. S. (2019). *Using multivariate statistics*. (7. Edition). Boston: Pearson Education.
- Tagle, F., Gómez, R., & Gamarra, R. (2024). Corruption and media surveillance of power in Argentina and Peru: The coverage of Clarín and El Comercio during the vaccination scandals against COVID 19. *Observatorio (OBS*)*, 18(3), 18-35. <https://doi.org/10.15847/obsOBS18320242411>
- Trottier, D. (2011). A research agenda for social media surveillance. *Fast Capitalism*, 8(1), 59-68. <https://doi.org/10.32855/fcapital.201101.008>
- Turow, J., Hennessy, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Philadelphia. <http://dx.doi.org/10.2139/ssrn.2820060>
- US Senate (2018). *Facebook, social media privacy, and the use and abuse of data: Joint full committee hearing*. Committee on the Judiciary. Retrived from <https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data>
- van der Schyff, K., & Flowerday, S. (2019). Social media surveillance: A personality-driven behaviour model. *South African Journal of Information Management*, 21(1), 1-9. <https://doi.org/10.4102/sajim.v21i1.1034>
- van der Schyff, K., Flowerday, S., & Furnell, S. (2020). Duplicitous social media and data surveillance: An evaluation of privacy risk. *Computers & Security*, 94, 1-17. <https://doi.org/10.1016/j.cose.2020.101822>
- van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, 78, 283-297. <https://doi.org/10.1016/j.chb.2017.10.007>
- Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication*, 17(1), 101-115. <https://doi.org/10.1111/j.1083-6101.2011.01559.x>
- We Are Social (2025). *Digital 2025*, Retrived from <https://wearesocial.com/uk/blog/2025/02/digital-2025-the-essential-guide-to-the-global-state-of-digital/>
- Wood, D. M., & Webster, C.W. R. (2009). Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research*, 5(2), 259-273. <https://doi.org/10.30950/jcer.v5i2.159>
- Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The internet privacy paradox revisited. *Information, Communication & Society*, 16(4), 479-500. <https://doi.org/10.1080/1369118X.2013.777757>
- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75-89. <https://doi.org/10.1057/jit.2015.5>