

DOI: https://doi.org/10.48009/4_iis_2024_118

Navigating Trust and Privacy: Contradictions and Insights in the Age of Social Media

Zoroayka V. Sandoval, *Middle Georgia State University*, vicky.sandoval@mga.edu

Neil J. Rigole, *Middle Georgia State University*, neil.rigole@mga.edu

Kembley Lingelbach, *Middle Georgia State University*, kembley.lingelbach@mga.edu

Abstract

As the use of social media platforms has become an integral part of daily life, the increased usage raises significant concerns regarding privacy, security, trust, and awareness. This quantitative study explores whether there were statistically significant differences between participant's concerns about privacy, security, trust, and awareness and their age, gender, social media usage, and their status (faculty, staff, undergraduate or graduate student) at the institution. Based on the results, there were significant differences found and they are discussed in this research paper.

Keywords: security, awareness, trust, privacy, social media

Introduction

Social media has become an integral part of daily life. However, this increased usage raises significant concerns of privacy, security, trust, and risk awareness. Despite the benefits of social media that include influencing communication, information sharing, and educational activities, there is growing anxiety among users regarding collection, storage, and usage of their personal information by these platforms. Previous studies have shown that users often feel they have lost control over their personal data and are skeptical about the security measures in place to protect their information (Liu, et al., 2022; Pew Research Center, 2023; Infosec Institute, 2018).

This widespread adoption of social media indicates a significant role that social media plays in modern communication and information dissemination. Addressing these concerns requires ongoing efforts to provide transparency, increase security measures, and educate users about best practices for protecting their personal information. These concerns also illuminate the importance of understanding how social media is used and perceived across different demographics, with respect to security, privacy, trust and risk awareness. Such insights can help inform better practices and policies to enhance the overall digital experience.

The aim of this study was to determine whether there were significant differences between the four independent variables of (1) age, (2) gender, (3) participant category, and (4) social media usage and the four dependent variables of the instrument (1) privacy concerns, (2) security concerns, (3) trust, and (4) risk awareness. The following four research questions were stated to be consistent with the purpose of this study:

RQ1: Are there significant mean differences between the independent variable of *age* and each of the four dependent variables of the instrument (privacy concerns, security concerns, trust, and risk awareness) separately?

RQ2: Are there significant mean differences between the independent variable of *gender* and each of the four dependent variables of the instrument (privacy concerns, security concerns, trust, and risk awareness) separately?

RQ3: Are there significant mean differences between the independent variable of *participant category* and each of the four dependent variables of the instrument (privacy concerns, security concerns, trust, and risk awareness) separately?

RQ4: Are there significant mean differences between the independent variable of *social media usage* and each of the four dependent variables of the instrument (privacy concerns, security concerns, trust, and risk awareness) separately?

Literature Review

For this study's purpose, we define privacy as the ability of individuals to control who has access to their personal information and how it is used, including managing the settings and information users share on social media. This differentiates from the concept of “risk awareness” which involves understanding and recognizing potential threats and vulnerabilities that could compromise privacy. Security, on the other hand, is being defined as measures and practices to protect data, accounts, and systems from unauthorized access, attacks, or harm. The discourse on privacy in the digital era necessitates an understanding of both domestic and international legal frameworks. Unlike the European Union, which has adopted the General Data Protection Regulation (GDPR) as a comprehensive approach to privacy, the United States lacks a unified federal privacy law. Instead, it has a patchwork of state-specific legislations, with only a handful of states like California, Virginia, Colorado, New York, and Washington enacting significant privacy policies (Bonta, 2023). This scenario underscores a critical gap in privacy protection across the nation, leaving the majority of Americans without adequate safeguards.

The advent of social media, and apps such as TikTok has introduced new challenges to privacy, highlighted by the ubiquity of End User License Agreements (EULAs) and the pervasive collection of data through internet cookies (Aziz & Telang, 2016; Ericson et al., 2022). Despite legislative efforts, the balance between convenience and privacy remains precarious, as consumers often acquiesce to privacy invasions for the sake of convenience (Obar & Oeldorf-Hirsch, 2020) even when there may be concerns that the user's private information could be shared against the individual's will.

Of all the varied social media apps, TikTok continues to come under scrutiny in the US. This has led many states and governors to ban the app on all government-owned or issued devices (such as cellphones and laptops) as well as banning it from the state's networks (Bunch, 2023; Morabito, 2023, Silver & Clancy, 2023). Despite the government bans and media attention, TikTok, originally known as Douyin when it was developed and released in China in 2016, continues to be one of the most popular apps worldwide. In March of 2023, Reuters reported that TikTok currently had 150 million US users, up from 100 million in 2020 (Shepardson, 2023) with Sprout Social predicting TikTok will grow to 2.2 billion users worldwide by 2027 (West, 2024).

While the United States federal and state governments grapple with how to address the national security

concerns of having such a popular app in the hands of so many its citizens, individuals have concerns of their own when it comes to their individual security, privacy, and awareness of their own personal data and social media activities.

For many social media users, if they are able to achieve something they want in return (i.e., social recognition) then they are more willing to share personal data (Fandia, 2019, p. 217). Privacy policies (containing information related to people's privacy and what data can be shared) for social media apps are typically ignored and accepted without reading their content (Ibdah, et.al., 2021). Also, all social media users are exposed to security issues like phishing, hijacking, and malware attacks and are potential risks for them (Kumar & Somani, 2018).

TikTok's massive growth has been fueled by collecting sensitive information and data about its users, even if they have not shared nor saved any content. (CISEsecurity.org, 2023). According to TikTok's policies, data that can be collected or accessed are usernames, ages, phone numbers, email address, details about the devices and mobile network being use, keystrokes, messages on the app and biometric information such as facial recognition prints, and voice prints according to the apps privacy policy (TikTok). TikTok's algorithm can also track the videos watched and how much time is spent on the video to track patterns and behavior so it can tailor content. TikTok's privacy policy was updated on May 22, 2023 (TikTok Privacy Policy, 2023).

Trust & Risk Awareness

The concept of trust is neither new nor exclusive to social media use, and empirical evidence regarding the impact of trust on privacy concerns is mixed. For instance, Chen, Beaudoin, and Hong (2016) found no significant relationship between trust and online privacy concerns in a sample of adolescents. In contrast, Bergström (2015) identified trust in others as "the single most important factor explaining privacy concerns among people using digital media and applications" (p. 425). Turow and Hennessy (2007) discovered that general trust in the Internet correlates with beliefs that institutions are more likely to help protect users' privacy and less likely to disclose sensitive information against their will. Additionally, Männiste and Masso (2018) found that trust in government, state, and media institutions significantly reduces concerns about institutional privacy violations. Furthermore, in both offline and online communication, trust is expected to mitigate the perceived risks associated with disclosing personal information, thereby reducing privacy concerns (Metzger, 2004). This notion aligns with Trepte's (2021) social media privacy model, which posits that trust, alongside interpersonal communication and norms, can replace the desire for control in social media usage.

Communication research has shown that many users perceive privacy threats as minimal or insignificant, often underestimating the risks or being overwhelmed by the benefits of online communication (Barth & de Jong, 2017). Some users dismiss privacy concerns entirely, believing they "have nothing to hide," a rather short-sighted view (Marwick & Hargittai, 2019; Solove, 2007, 2011). However, incidents such as the Cambridge Analytica data-mining scandal and Edward Snowden's revelations about mass surveillance have made Internet users more aware and potentially more concerned about privacy (Blank, et al., 2019; Madden & Rainie, 2015; Paine, et al., 2007). Research involving interviews with 54 adolescents in Switzerland suggested that adolescents are aware of online privacy related to their social connections and consciously manage their privacy. However, TikTok's algorithm and its popularity among peers can pose risks. Adolescents also share TikToks on private channels like Snapchat to control who sees their posts and avoid identification. Moreover, they use multiple accounts with different privacy settings to manage their content (Ebert, et al., 2023, p. 1).

Methodology

An instrument designed to measure users' privacy concerns, security concerns, trust and risk awareness on social media was used in this study. The instrument was developed by Koohang, Floyd, Yerby, and Paliszkievicz (2021), and is composed of 4 constructs: (1) privacy concerns (4 questions), (2) security concerns (5 questions), (3) trust (3 questions), and (4) risk awareness (3 questions) with a total of 15 questions. A 7-point Likert scale ranging from 7 - Completely Agree and 1 - Completely Disagree was used to collect data. The instrument was found to be reliable; a Bartlett's Test of Sphericity was performed, and the results indicated a validity of $p = 0.000$ (Koohang, et.al., 2021). Also, demographic questions, such as age, gender, social media platforms used, and their status at the institution were collected.

Data Collection

Once the Institutional Review Board (OHRP, 2021) approved this research, a convenience sample was used to select participants. A link to the survey was sent via email to all faculty, staff members, and Information Technology students at a university in the Southeast USA. Information Technology students were enrolled in undergraduate, masters, or doctoral level courses. After the first email was sent, the link was re-sent 2 weeks later for 25 days (about 3 and a half weeks) of data collection. A total of 113 responses were collected during the data collection period. One response was removed because it was not complete; therefore, the sample consisted of 112 responses for this study. From the sample ($N=112$), 41.07% were male ($N=46$) and 58.92% were female ($N=66$). Participants' age was grouped in the following categories: 18-25 ($N=10$; 8.93%), 26-35 ($N=19$; 16.96%), 36-45 ($N=38$; 33.93%), 46-55 ($N=30$; 26.79%), 56-65 ($N=12$; 10.71%), and over 65 ($N=3$; 2.68%).

Data Analysis

One-way ANOVAs were conducted to test significance of groups' differences and analyze data collected for each of the four research questions (RQ1, RQ2, RQ3, and RQ4). To determine significance of the groups, F test was used. For groups with more than two levels, post-hoc analysis was conducted using the Tukey HSD test. In this study, four independent variables were included: (1) age, (2) gender, (3) participant category, and (4) social media usage. The four dependent variables were: (1) privacy concerns, (2) security concerns, (3) trust, and (4) risk awareness.

Results

As part of the questions, participants were asked how they identified at the institution, as well as the social media platforms they used. Table 1 shows the categories that participants reported. Note that, of the 4 categories, undergraduate students and graduate students are Information Technology majors, while staff and faculty are from all disciplines at the institution. We can see that undergraduate students, staff and faculty have a similar participation, ranging from 29 to 33 participants, while graduate students were only 20 participants. This is not surprising since the IT graduate students' population is smaller. Overall results for the social media platforms used are shown in Table 2. In Table 3, we can see the social media platforms usage by category. Overall, the three most used social media platforms are Facebook, LinkedIn, and Instagram. The most used social media platforms (70% or more) by undergraduate students are Facebook and LinkedIn; by graduate students are Facebook, LinkedIn, and Instagram; and by staff and faculty members is Facebook.

Table 1: Participant category

Participant Category	Percent	Cumulative %
Undergraduate student	26.8 %	26.8 %
Graduate student	17.9 %	44.7 %
Staff	29.5 %	74.1 %
Faculty	25.9 %	100 %

Table 2: Overall social media platform usage

Social Media platform	%
Facebook	83.9 %
LinkedIn	68.1 %
Instagram	61.9 %
Twitter/X	49.6 %
Pinterest	40.7 %
Reddit	38.9 %
TikTok	30.1%
SnapChat	22.1 %
Other	10.6 %
Tumblr	8.8 %
Flickr	3.5 %
None	2.7 %
Vine	0.9 %

Table 3: Social media platform usage per category

Social Media platform	Undergraduate students N=30	Graduate students N=20	Staff N=33	Faculty N=29
Facebook	21 (70%)	18 (90%)	28 (85%)	27 (93%)
LinkedIn	21 (70%)	16 (80%)	22 (67%)	18 (62%)
Instagram	19 (63%)	16 (80%)	21 (64%)	14 (48%)
Twitter/X	18 (60%)	11 (55%)	16 (48%)	11 (38%)
Pinterest	11 (37%)	6 (30%)	19 (58%)	10 (34%)
Reddit	16 (53%)	8 (40%)	11 (33%)	9 (31%)
TikTok	11 (37%)	4 (20%)	17 (52%)	2 (7%)
SnapChat	8 (27%)	5 (25%)	10 (30%)	2 (7%)
Other	4 (13%)	2 (10%)	3 (9%)	3 (10%)
Tumblr	2 (7%)	1 (5%)	7 (21%)	0 (0%)
Flickr	3 (10%)	0 (0%)	1 (3%)	0 (0%)
None	1 (3%)	1 (5%)	1 (3%)	0 (0%)
Vine	0 (0%)	0 (0%)	1 (3%)	0 (0%)

Results of the descriptive analyses are shown in Table 4. Participants revealed more agreement to the questions related to privacy concerns, risk awareness, and security concerns, however, a neutral position was revealed for questions about trust.

Table 4: Means and Standard Deviations

	Mean	Std. Deviation
Privacy concerns	5.8876	1.16203
Security concerns	5.0165	1.50803
Trust	3.4107	1.29524
Risk Awareness	6.1280	0.91724

RQ1: Are there significant mean differences between the independent variable of age and each of the four dependent variables of the instrument (privacy concerns, security concerns, trust, and risk awareness) separately?

Results of the ANOVA for RQ1 revealed no significant difference between age and the constructs of Privacy Concerns ($F_{5,106}=.980$, $p=.434$), Security Concerns ($F_{5,106}=.877$, $p=.499$), Trust ($F_{5,106}=.314$, $p=.903$) and Risk Awareness ($F_{5,106}=.863$, $p=.508$). Results of ANOVA are shown in Table 5, and descriptive statistics in Table 6.

Table 5: ANOVA Results for Age

		Sum of Squares	df	Mean Square	F	Sig.
Privacy	Between Groups	6.622	5	1.324	0.980	0.434
	Within Groups	143.263	106	1.352		
	Total	149.885	111			
Security	Between Groups	10.029	5	2.006	0.877	0.499
	Within Groups	242.403	105	2.287		
	Total	252.432	111			
Trust	Between Groups	2.720	5	0.544	0.314	0.903
	Within Groups	183.498	106	1.731		
	Total	186.218	111			
Awareness	Between Groups	3.655	5	0.731	0.863	0.508
	Within Groups	89.733	106	0.847		
	Total	93.388	111			

Table 6.: Descriptive Statistics for Age

		N	Mean	Std. Deviation
Privacy	18-25	10	5.3250	1.62895
	26-35	19	5.9079	1.16729
	36-45	38	6.0395	1.14863
	46-55	30	5.7389	1.06982
	56-65	12	6.2708	1.03605
	over 65	3	5.6667	0.72169
	Total	112	5.8876	1.16203
Security	18-25	10	4.5800	1.61507
	26-35	19	4.5474	1.74845
	36-45	38	5.2842	1.41317
	46-55	30	4.9817	1.55422
	56-65	12	5.3167	1.17073
	over 65	3	5.2000	1.56205
	Total	112	5.0165	1.50803
Trust	18-25	10	3.4667	1.07955
	26-35	19	3.0877	1.33723
	36-45	38	3.4123	1.40875
	46-55	30	3.5333	1.29129
	56-65	12	3.5556	1.05728
	over 65	3	3.4444	1.83586
	Total	112	3.4107	1.29524
Awareness	18-25	10	6.6000	0.56218
	26-35	19	6.1404	0.89798
	36-45	38	6.0702	0.92726
	46-55	30	5.9556	1.13033
	56-65	12	6.3056	0.48113
	over 65	3	6.2222	0.69389
	Total	112	6.1280	0.91724

RQ2: Are there significant mean differences between the independent variable of gender and each of the four dependent variables of the instrument (privacy concerns, security concerns, trust, and risk awareness) separately?

Results of the ANOVA for RQ2 revealed no statistically significant difference between gender and the constructs of Privacy Concerns ($F_{1,110}=.181$, $p=.672$), Security Concerns ($F_{1,110}=.002$, $p=.969$), Trust ($F_{1,110}=.259$, $p=.612$) and Risk Awareness ($F_{1,110}=.624$, $p=.431$). Results of ANOVA are shown in Table 7, and descriptive statistics in Table 8.

Table 7: ANOVA Results for Gender

		Sum of Squares	df	Mean Square	F	Sig.
Privacy	Between Groups	0.246	1	0.246	0.181	0.672
	Within Groups	149.639	110	1.360		
	Total	149.885	111			
Security	Between Groups	0.004	1	0.004	0.002	0.969
	Within Groups	252.428	110	2.295		
	Total	252.432	111			
Trust	Between Groups	0.437	1	0.437	0.259	0.612
	Within Groups	185.782	110	1.689		
	Total	186.218	111			
Awareness	Between Groups	0.527	1	0.527	0.624	0.431
	Within Groups	92.861	110	0.844		
	Total	93.388	111			

Table 8: Descriptive Statistics for Gender

		N	Mean	Std. Deviation
Privacy	Male	46	5.8315	1.28458
	Female	66	5.9268	1.07691
	Total	112	5.8876	1.16203
Security	Male	46	5.0098	1.45890
	Female	66	5.0212	1.55242
	Total	112	5.0165	1.50803
Trust	Male	46	3.4855	1.35119
	Female	66	3.3586	1.26263
	Total	112	3.4107	1.29524
Awareness	Male	46	6.2101	0.82957
	Female	66	6.0707	0.97580
	Total	112	6.1280	0.91724

RQ3: Are there significant mean differences between the independent variable of participant category and each of the four dependent variables of the instrument (privacy concerns, security concerns, trust, and risk awareness) separately?

Results of the ANOVA for RQ3 revealed a statistically significant difference between participant category and Risk Awareness using social media ($F_{3,108}=3.527$, $p=.017$). Post hoc comparisons using the Tukey HSD test indicated that the mean score of risk awareness for participants that identified as undergraduate

students ($M=6.55$, $SD=.657$) was significantly different than the score of risk awareness for participants that identified as staff ($M=5.85$, $SD=1.09$). No significant difference was found among participants from other participant categories. Results of ANOVA for participant category are shown in Table 9, and descriptive statistics in Table 10.

Table 9: ANOVA Results for Participant Category

		Sum of Squares	df	Mean Square	F	Sig.
Privacy	Between Groups	0.179	3	0.060	0.043	0.988
	Within Groups	149.706	108	1.386		
	Total	149.885	111			
Security	Between Groups	3.886	3	1.295	0.563	0.641
	Within Groups	248.546	108	2.301		
	Total	252.432	111			
Trust	Between Groups	1.009	3	0.336	0.196	0.899
	Within Groups	185.209	108	1.715		
	Total	186.218	111			
Awareness	Between Groups	8.333	3	2.778	3.527	0.017
	Within Groups	85.055	108	0.788		
	Total	93.388	111			

Table 10: Descriptive Statistics for Participant Category

		N	Mean	Std. Deviation
Privacy	Undergraduate student	30	5.9000	1.27746
	Graduate student	20	5.9625	1.26511
	Staff	33	5.8485	1.05871
	Faculty	29	5.8678	1.13554
	Total	112	5.8876	1.16203
Security	Undergraduate student	30	5.1267	1.46827
	Graduate student	20	4.9700	1.61477
	Staff	33	4.7591	1.56951
	Faculty	29	5.2276	1.43500
	Total	112	5.0165	1.50803

		N	Mean	Std. Deviation
Trust	Undergraduate student	30	3.3000	1.42863
	Graduate student	20	3.3167	1.50428
	Staff	33	3.4747	1.10877
	Faculty	29	3.5172	1.24908
	Total	112	3.4107	1.29524
Awareness	Undergraduate student	30	6.5556	0.65702
	Graduate student	20	6.0667	0.86923
	Staff	33	5.8485	1.09001
	Faculty	29	6.0460	0.84855
	Total	112	6.1280	0.91724

There was no statistically significant difference between the participant category and privacy concerns ($F_{3,108}=.043$, $p=.988$), security concerns ($F_{3,108}=.563$, $p=.641$), and trust ($F_{3,108}=.196$, $p=.899$).

RQ4: Are there significant mean differences between the independent variable of social media usage and each of the four dependent variables of the instrument (privacy concerns, security concerns, trust, and risk awareness) separately?

Results of the ANOVA for RQ4 revealed a statistically significant difference between social media usage and risk awareness ($F_{3,108}=3.66$, $p=.015$). Post hoc comparisons using the Tukey HSD test indicated that the mean score of risk awareness for participants using 7-9 social media platforms ($M=6.52$, $SD=.547$) was significantly different than the score of risk awareness for participants using 1-3 social media platforms ($M=6.07$, $SD=.764$). Results of ANOVA for social media usage are shown in Table 11, and descriptive statistics in Table 12.

Table 11. ANOVA Results for Social Media Usage

		Sum of Squares	df	Mean Square	F	Sig.
Privacy	Between Groups	6.238	3	2.079	1.563	0.202
	Within Groups	143.647	108	1.330		
	Total	149.885	111			
Security	Between Groups	6.205	3	2.068	0.907	0.440
	Within Groups	246.227	108	2.280		
	Total	252.432	111			

		Sum of Squares	df	Mean Square	F	Sig.
Trust	Between Groups	5.987	3	1.996	1.196	0.315
	Within Groups	180.231	108	1.669		
	Total	186.218	111			
Awareness	Between Groups	8.629	3	2.876	3.665	0.015
	Within Groups	84.759	108	0.785		
	Total	93.388	111			

Table 12: Descriptive Statistics for Social Media Usage

		N	Mean	Std. Deviation
Privacy	None	3	6.5000	0.66144
	1-3 SM platforms	42	6.1111	1.04435
	4-6 SM platforms	48	5.8021	1.20500
	7-9 SM platforms	19	5.5132	1.28688
	Total	112	5.8876	1.16203
Security	None	3	5.3333	1.30128
	1-3 SM platforms	42	5.2810	1.39690
	4-6 SM platforms	48	4.9052	1.51721
	7-9 SM platforms	19	4.6632	1.74235
	Total	112	5.0165	1.50803
Trust	None	3	2.3333	1.52753
	1-3 SM platforms	42	3.6190	1.45682
	4-6 SM platforms	48	3.2917	1.14777
	7-9 SM platforms	19	3.4211	1.21636
	Total	112	3.4107	1.29524
Awareness	None	3	4.7778	1.95316
	1-3 SM platforms	42	6.0794	0.76442
	4-6 SM platforms	48	6.0972	1.00814
	7-9 SM platforms	19	6.5263	0.54790
	Total	112	6.1280	0.91724

Discussion

The study examined the relationship between social media usage and risk awareness, as well as privacy concerns, security concerns, and trust, across different demographics. It found that while increased exposure to multiple social media platforms significantly heightened users' risk awareness, it did not affect their overall privacy concerns, security concerns, or trust levels. Older participants exhibited slightly higher

levels of privacy concerns and risk awareness compared to younger participants, likely due to their greater experience with social media risks. No significant differences were found between male and female participants regarding privacy, security, trust, and risk awareness, indicating that gender does not significantly influence these perceptions. However, undergraduate students, particularly those studying Information Technology, reported significantly higher risk awareness than staff members, likely due to their educational environment. Overall, the study suggests that while heavy social media users are more aware of risks, their concerns about privacy, security, and trust remain consistent with those of lighter users. These findings highlight the need for targeted educational and policy approaches to address specific concerns among different user groups.

Conclusion

In conclusion, this study highlights the nuanced nature of privacy, security, trust, and risk awareness concerns across different demographics and social media usage patterns. The significant findings regarding participant category and social media usage suggest targeted approaches in educational and policy-making efforts to address specific concerns among different user groups. Future research could further explore these dynamics to develop more effective strategies for enhancing digital experiences and safeguarding user privacy and security on social media platforms.

This study aimed to assess perceptions of privacy, security, risk awareness, and trust related to social media usage across different demographic groups, including age, gender, higher education students, faculty, and staff. The findings indicated a notable concern for privacy, security, risk awareness, and trust among participants. Interestingly, the study revealed that undergraduate IT students who used between seven and nine social media platforms exhibited significantly higher levels of concern compared to other groups. This may be attributed to their increased exposure to various platforms in their academic pursuits.

Based on these findings, several actionable recommendations can be made to enhance the digital experience for users: 1) Institutions should implement comprehensive training programs focusing on digital literacy, emphasizing privacy, and security best practices. This is particularly important for students and staff who use multiple social media platforms; 2) Organizations should develop and enforce robust privacy and security policies. These policies must be clearly communicated to all users, ensuring they understand the importance of protecting their personal information; and 3) Social media platforms should offer more intuitive and accessible privacy settings. Simplifying the process of managing privacy preferences can help users feel more in control of their information.

References

- Aziz, A., & Telang, R. (2016). What is a digital cookie worth? *Social Science Research Network*.
<http://dx.doi.org/10.2139/ssrn.2757235>
- Barth, S., & de Jong, M. D. (2017). The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. doi:10.1016/j.tele.2017.04.013
- Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 53, 419–426.
doi:10.1016/j.chb.2015.07.025

- Blank, G. & Dutton, W. H., & Lefkowitz, J. (2019). Perceived threats to privacy online: The Internet in Britain. Oxford Internet Survey 2019. Oxford Internet Institute, University of Oxford. Retrieved from <https://oxis.oii.ox.ac.uk/wp-content/uploads/sites/16/2019/09/OxIS-report-2019-finaldigital-PDFA.pdf>.
- Bonta, R. (2023, May 10). California consumer privacy act (CCPA). State of California Department of Justice. <https://oag.ca.gov/privacy/ccpa>
- Bunch, R. (2022, December 15). Kemp bans use of TikTok on state agency devices. Georgia Public Broadcasting. <https://www.gpb.org/news/2022/12/15/kemp-bans-use-of-tiktok-on-state-agencydevices> [<https://perma.cc/XSW7-TZ8U>]
- CISEsecurity.org (2023). TikTok: Influence Ops, Data Practices Threaten US Security. The Cyber Threat Intelligence (CTI) team at the Multi-State Information Sharing and Analysis Center. <https://www.cisecurity.org/insights/blog/tiktok-influence-ops-data-practices-threaten-us-security>
- Chen, H., Beaudoin, C. E., & Hong, T. (2016). Teen online information disclosure: Empirical testing of a protection motivation and social capital model. *Journal of the Association for Information Science and Technology*, 67(12), 2871–2881. doi:10.1002/asi.23567
- DataReportal (2024). 5 Billion Social Media Users. Retrieved from <https://datareportal.com/reports/digital-2024-deep-dive-5-billion-social-media-users>
- Ebert, N., Geppert, T., Strycharz, J., Knieps, M., Hönig, M., & Brucker-Kley, E. (2023). Creative beyond TikToks: Investigating adolescents' social privacy management on TikTok. *arXiv preprint arXiv:2301.11600*.
- Ericson, D. J., Albert, S. W., Bernard, P. B., & Brown, E. (2022). End-User license agreements (EULAs): Investigating the impact of human-centered design on perceived usability, attitudes, and anticipated behavior. *Information Design Journal*, 26(3). 190-208. <https://doi.org/10.1075/idj.20018.eri>
- Fandia, M. P. (2019). Privacy and Social Media: Defining privacy in the usage of path. The 10th IGSSCI, KnE Social Sciences, pp. 217–235. DOI 10.18502/kss.v3i20.4938
- Ibdah, D., Lachtar, N., Raparathi, S. M. & Bacha, A. (2021). Why should I read the privacy policy, I just need the service”: A study on attitudes and perceptions toward privacy policies. *IEEE Access*, vol. 9, pp. 166465-166487, 2021, doi: 10.1109/ACCESS.2021.3130086.
- Infosec Institute (2018). Security awareness in higher education. <https://www.infosecinstitute.com/resources/security-awareness/security-awareness-in-higher-education/>
- Koohang, A., Floyd, K., Yerby, J., & Paliszkievicz, J. (2021). Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. *Issues in Information Systems*, 22(2), pp. 133-145. DOI: https://doi.org/10.48009/2_iis_2021_136-149
- Kumar, S. and Somani, V. (2018). Social media security risks, cyber threats and risks prevention and mitigation techniques. *IJSART*, 4(4). <https://www.researchgate.net/profile/Sunil-Kumar->

310/publication/324860729_Social_Media_Security_Risks_Cyber_Threats_And_Risks_Prevention_And_Mitigation_Techniques/links/5ae7e97fa6fdcc03cd8dbf84/Social-Media-Security-Risks-Cyber-Threats-And-Risks-Prevention-And-Mitigation-Techniques.pdf

- Liu, Y., Tse, W. K., Kwok, P. Y., & Chiu, Y. H. (2022). Impact of social media behavior on privacy information security based on analytic hierarchy process. *Information*, 13(6), 280.
- Madden, M., & Rainie, L. (2015, May 20). *Americans' attitudes about privacy, security and surveillance*. Pew Research Center. Retrieved from <http://www.pewinternet.org/2015/05/20/americansattitudes-about-privacy-security-and-surveillance/>
- Männiste, M., & Masso, A. (2018). The role of institutional trust in Estonians' privacy concerns. *Studies of Transition States and Societies*, 10(2), 22–39.
- Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, 22(12), 1697–1713. doi:10.1080/1369118X.2018.1450432
- Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-mediated Communication*, 9(4). doi:10.1111/j.1083-6101.2004.tb00292.x
- Morabito, A. (2023, January 23). Get TikTok off public-funded education devices. Washington Examiner. <https://www.washingtonexaminer.com/policy/education/2738292/get-tiktok-off-public-funded-education-devices>
- Obar, J. & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*. 23(1), 128-147. <https://doi.org/10.1080/1369118X.2018.1486870>
- Office for Human Research Protections (OHRP). (2021, June 28). *Lesson 3: What are irbs?*. HHS.gov. <https://www.hhs.gov/ohrp/education-and-outreach/online-education/human-research-protection-training/lesson-3-what-are-irbs/index.html>
- Paine, C., Reips, U. D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of privacy concerns' and 'privacy actions.' *International Journal of Human-Computer Studies*, 65(6), 526–536. doi:10.1016/j.ijhcs.2006.12.001
- Pew Research Center (2023). Protecting both privacy and security in higher ed. Retrieved from <https://edtechmagazine.com/higher/article/2021/08/protecting-both-privacy-and-security-higher-ed>
- Silver, L. & Clancy, L. (2023, March 31). *By more than two-to-one, Americans support U.S. government banning TikTok*. Pew Research Center. <https://www.pewresearch.org/short-reads/2023/03/31/by-a-more-than-two-to-one-margin-americans-support-us-government-banning-tiktok/>
- Shepardson, D. (2023, March 20). TikTok hits 150 mln U.S. monthly users, up from 100 million in 2020. *Reuters*. <https://www.reuters.com/technology/tiktok-tell-congress-it-has-150-million-monthly-active-us-users-2023-03-20>

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, 44, 745–772.

Solove, D. J. (2011, May 15). Why privacy matters even if you have “nothing to hide.” *The Chronicle of Higher Education*. Retrieved from <http://chronicle.com/article/Why-Privacy-Matters-Evenif/127461/>

TikTok Privacy Policy (2023, May 22). Privacy Policy. Independently Published. <https://www.tiktok.com/legal/page/us/privacy-policy/en>

Trepte, S. (2021). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory*, 31(4), 549–570. doi:10.1093/ct/qtz035

Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust: Insights from a national survey. *New Media & Society*, 9(2), 300–318. doi:10.1177/1461444807072219

West, C. (2024, February 20). 27 TikTok statistics marketers need to know in 2024. *Sprout Social*. <https://sproutsocial.com/insights/tiktok-stats/>