Navigating Social Media Privacy: Awareness, Preferences, and Discoverability

Pithayuth Charnsethikul
University of Southern California Information Sciences Institute
charnset@usc.edu

Almajd Zunquti
University of Southern California Information Sciences Institute
zunquti@usc.edu

Gale Lucas
University of Southern California Institute for Creative Technologies
lucas@ict.usc.edu

Jelena Mirkovic
University of Southern California Information Sciences Institute
mirkovic@isi.edu

Abstract

Social media platforms provide various privacy settings, which users can adjust to fit their privacy needs. Platforms claim that this is sufficient – users have power to accept the default settings they like, and change those they do not like. In this paper, we seek to quantify user awareness of, preferences around and ability to adjust social media privacy settings. We conduct an online survey of 541 participants across six different social media platforms: Facebook, Instagram, X, LinkedIn, TikTok, and Snapchat. We focus on nine privacy settings that are commonly available across these platforms, and evaluate participants' preferences for privacy, awareness of the privacy settings and ability to locate them. We find that default settings are ill-aligned with user preferences – 92% of participants prefer at least one of the privacy options to be more private than the default. We further find that users are generally not aware of privacy settings, and struggle to find them. 80% of participants have never seen at least one privacy setting, and 79% of participants rated at least one setting as hard to find. We also find that the fewer privacy settings a user has seen, the harder for them to locate those settings, and the higher the level of privacy they desire. Additionally, we find that there are significant differences in privacy setting preferences and usability across different user age groups and across platforms. Older users are more conservative about their privacy, they have seen significantly fewer privacy settings, and they spend significantly more time locating them than younger users. On some platforms, like LinkedIn, users opt for higher visibility, while on others they prefer more privacy. Some platforms, like TikTok, make it significantly easier for users to locate privacy settings. Based on our findings, we provide recommendations on default values and how to improve usability of privacy settings on social media.

Keywords

Privacy, Social Media, Awareness, Default Privacy Settings

Proceedings on Privacy Enhancing Technologies 2025(4), 620–638

https://doi.org/10.56553/popets-2025-0148

1 Introduction

Social media platforms have been around for decades, with more than 60% of the world's population now being social media users [62]. As these platforms continue to grow, privacy concerns among users have increased [4, 24, 39], as has frequency of privacy incidents. In 2018, Cambridge Analytica harvested data from up to 87 million Facebook users without their consent, and used this data for targeted political advertising [59]. In 2021, LinkedIn faced a significant data scraping incident, where publicly visible profile details from around 700 million users were scraped and sold on dark web [64]. In the same year, U.S. President Joe Biden's Venmo account was discovered through an app search tool, leading to an exposure of his family members and White House officials, due to his publicly visible friend list [27]. In all these cases, the default settings of the platform exposed specific user information without their knowledge and explicit consent.

To address privacy concerns, platforms provide various privacy settings, which users can customize to align them with their privacy needs. For example, most platforms allow users to customize which of their private information can be used for targeted ads or whether they want to receive targeted ads [14, 58]. Additionally, Facebook and LinkedIn offer privacy settings that allow users to adjust visibility of their profile details (e.g., education, job, location) and control who can see their friend lists. Platforms claim that providing these settings will sufficiently empower users to control and protect their own privacy [3, 57].

But simply providing the privacy settings to users is not enough! If users are unaware that these settings exist [25, 53, 56], or if they struggle to find [20] and understand them [50], then users cannot adjust the settings to meet their privacy needs. These challenges lead users to continue using the default privacy options, which are typically set to be more exposed than users prefer [44, 45, 63].

1.1 Contributions

In this paper, we seek to quantify the need for and usability of social media privacy settings across six different social media platforms, including Facebook, Instagram, X, LinkedIn, TikTok, and Snapchat. We focus on these platforms due to their widespread popularity [61]. Unlike previous studies [30, 34, 44, 45, 47] on social media privacy settings, which usually focused on a single platform, our study of multiple platforms enables us to gain a broader understanding of social media users' privacy preferences, including perspectives that

are shared across platforms (e.g., what type of information users prefer to keep private on any platform) and those that are unique to a given platform. We focus on nine privacy settings that are commonly available across our chosen six platforms.

We aim to answer the following research questions:

RQ1: What fraction of users have never seen a given privacy setting (**awareness**)?

RQ2: What fraction of users prefer higher privacy than the default for a given setting (**preferences**)?

RQ3: What fraction of users feel that a given privacy setting is hard to locate (**discoverability**)?

RQ4: Are there positive or negative correlations among awareness, preferences and discoverability (**correlations**)?

RQ5: Are there any demographic, usage, or platform-specific differences associated with awareness, preferences, and discoverability? (**differences**)?

We conducted an online survey with 541 participants, evenly distributed across age groups, platforms and genders. For each privacy setting, we asked participants if they have seen it, if they were satisfied with the default value, and if they could locate the setting on the platform. We measured the time taken to locate each setting, and asked the participant to rate the difficulty of this task.

We summarize our findings. First, *platforms' default settings are generally more exposed than what users prefer*, which was also found in prior work [44, 45]. In our study, 92% of participants prefer at least one of the privacy settings to be more private than the default, and 83% prefer multiple settings to be more private. Second, *users are generally unaware of some privacy settings*. 80% of our study participants have never seen at least one privacy setting, and 58% have never seen multiple settings. Third, *users struggle to find and adjust privacy settings*. 79% of our study participants feel that at least one privacy setting is hard to locate and 50% feel that multiple are hard to locate. Fourth, *there are significant correlations among awareness, preferences and discoverability*. We found that the fewer privacy settings a user has seen, the harder for them to locate those settings. Users who experience more difficulty locating privacy settings are the ones who prefer more privacy. Fifth, *there are significant differences in awareness of and ease of finding privacy settings across different age groups and across platforms*. In our study, older participants had seen significantly fewer privacy settings and spent significantly more time locating them than younger participants. Further, TikTok users find their privacy settings significantly easier to locate compared to other platforms.

Based on our findings, we make the following recommendations. First, platforms should better align their default settings with user preferences by choosing "friends only" as the default value. This would protect the majority of users from the start, while others, who desire more or less exposure can adjust the platform's privacy settings accordingly. Second, because many users struggle to find specific privacy settings, we recommend that platforms use precise wording to describe the settings and avoid placing them in misleading sections. Platforms could further greatly improve usability of their privacy settings if they worked together to develop a consistent set of options, wordings and setting placements across their user interfaces. Third, we highlight the need for regulators to step in to develop and enforce privacy guidelines and usability standards for social media platforms, ensuring stronger and more consistent privacy protections for users.

2 Background and Related Work

The usability of social media privacy settings has been extensively studied. Table 2 provides a summary of our comparison with related work. We first present related work, and then compare our work and highlight its novelty.

2.1 Privacy Awareness

Social media platforms assume that simply offering privacy settings is sufficient to protect user privacy. However, users are often unaware of available privacy settings or struggle to make optimal long-term privacy decisions due to cognitive limitations [3, 5, 9, 12, 23, 47, 48, 51, 53, 56–58]. As a result, they may not fully understand the privacy settings or the extent of their exposure [25, 55–57, 65].

Previous work usually studied users' unawareness by measuring the extent to which one privacy setting – "post audience" – were incorrectly adjusted. Liu et al. measured the number of users' posts where their actual audience did not match the users' desired audience on Facebook [44]. They asked for participants' permission to collect the actual audiences from a set of randomly selected posts, and then asked participants to specify their desired audience. Madejski et al. applied this approach to measure the post audience mismatch on Facebook with Columbia students [46, 47]. Both studies showed that the majority of Facebook post audiences were mismatched. Liu et al. reported that 67% of users' post audiences were incorrectly adjusted, while Madejski et al. found that every student had at least one post with a mismatched audience. Both studies also found that when mismatches occurred, users' posts were actually more exposed than what users expected.

Mondal et al. conducted a longitudinal study on post audiences from 2009 to 2018 and found that 65% of users wanted to change the audience for at least one of their posts during that period [48]. Recently, Lowens et al. expanded the mismatch study beyond the post audience setting to include other privacy settings (e.g., activity status, ads) on Facebook. Consistent with other previous work, they found that every participant had at least one mismatch across different privacy settings and, once again, most believed their actual settings were more restrictive than they actually were.

In addition to mismatch measurements, researchers have assessed users' unawareness by directly asking users if they were aware of specific privacy settings or when their information is being collected. Tuunainen et al. used this direct questioning approach and found that 73% of users were unaware that Facebook shared their information with third parties outside the platform [65]. Aljohani et al. applied this approach to users across Facebook, Instagram, Twitter, and Snapchat, and found that 66.4% of them were unaware of targeted ads [7]. Similarly, an empirical study by the Pew Research Center reported that 74% of users did not know about the targeted ads setting on Facebook.

2.2 Default Privacy Settings

When users are unaware of the privacy settings, their settings remain at the default. Some previous studies have also explored user

Table 1: Privacy settings available on each platform, with their descriptions, default values, and UI paths (Figure 4) constructed on iOS in November 2024. Friend+: friends and people from your phone contacts.

Privacy Settings	*Description*	*Platform*	*Default*	*UI-path (#clicks)*
audience	Who can see your posts?	Facebook	Friends	Menu, Settings & privacy, Posts (3)
		LinkedIn	Friends	Create a post, Who can see your post? (2)
		Snapchat	Friends	Profile, Settings, View my story (3)
	Is your account public or private?	Instagram	Public	Profile, Settings and activity, Account privacy (3)
		X	Public	Profile, Settings and privacy, Privacy and safety, Audience and tagging, Protect your posts (5)
		TikTok	Public	Profile, Settings and privacy, Privacy, Private account (4)
message	Who can send you messages?	Facebook	Anyone	Menu, Settings & privacy, How people find and contact you, How you get message requests (4)
		Instagram	Anyone	Profile, Settings and activity, Messages and story replies, Message requests (4)
		X	Friends	Profile, Settings and privacy, Privacy and safety, Direct messages (4)
		LinkedIn	Anyone	Profile, Settings, Data Privacy, Messages (4)
		TikTok	Friends	Profile, Settings and privacy, Privacy, Direct messages (4)
		Snapchat	Friends+	Profile, Settings, Contact me (3)
ads	Do you allow personalized ads?	Facebook	Yes	Menu, Settings & privacy, Account center, Ad preferences, Manage info (5)
		Instagram	Yes	Profile, Settings and activity, Account center, Ad preferences, Manage info (5)
		X	Yes	Profile, Settings and privacy, Privacy and safety, Ad preferences (4)
		LinkedIn	Yes	Profile, Settings, Advertising data, Third-party data (4)
		TikTok	Yes	Profile, Settings and privacy, Ads (3)
		Snapchat	Yes	Profile, Settings, Ads preferences (3)
activity status	Do you allow people to see when you are online?	Facebook	Yes	Menu, Settings & privacy, Active status (3)
		Instagram	Yes	Profile, Settings and activity, Messages and story replies, Show activity status (4)
		LinkedIn	Yes	Profile, Settings, Visibility, Manage active status (4)
		TikTok	Yes	Profile, Settings and privacy, Privacy, Activity status (4)
		Snapchat	Yes	Profile, Settings, Activity indicator (3)
account suggestion	Do you allow your account to be suggested to other users via phone number or email?	Facebook	Yes	Menu, Settings & privacy, How people find and contact you, Who can Facebook suggested your profile to ... (4)
		X	Yes	Profile, Settings and privacy, Privacy and safety, Discoverability and contacts, Let other find you by ... (5)
		LinkedIn	Yes	Profile, Settings, Visibility, Profile discovery using ... (4)
		TikTok	Yes	Profile, Settings and privacy, Privacy, Suggested your account to others (4)
		Snapchat	Yes	Profile, Settings, Mobile number/Email, Let others find me using my ... (4)
connection view	Who can see your friends list?	Facebook	Anyone	Menu, Settings & privacy, How people find and contact you, Who can see your friends list (4)
		LinkedIn	Friends	Profile, Settings, Visibility, Who can see your connections (4)
		TikTok	Anyone	Profile, Settings and privacy, Privacy, Following list (4)
video	Do you allow people to download your videos?	Instagram	Yes	Menu, Settings & privacy, Sharing and reuse, Downloads (4)
		X	Yes	Profile, Settings and privacy, Privacy and safety, Audience and tagging, Protect your videos (5)
		TikTok	Yes	Profile, Settings and privacy, Privacy, Downloads (4)
profile view	Who can see your profile details (e.g., education, location)?	Facebook	Anyone	Menu, Settings & privacy, Profile details (3)
		LinkedIn	Anyone	Profile, Settings, Visibility, Edit your public profile (4)
search engine	Do you allow your account to be linked to search engines?	Facebook	Yes	Menu, Settings & privacy, How people find and contact you, Do you want search engines to link to your profile? (4)
		LinkedIn	Yes	Profile, Settings, Visibility, Edit your public profile, Your profile's public visibility (5)

preferences concerning these default settings, and found that default settings are generally more exposed than users expect [2, 6, 18, 44, 68]. Pew Research Center found that 51% of Facebook users were not satisfied with its default ads practices [18]. Lowens et al. found that Facebook's default settings are generally more exposed than what users prefer [45]. For example, the default privacy setting for *account suggestion* on Facebook enables anyone to find your account via your phone number or email. However, Facebook users often expect this default setting to be disabled. Our initial survey of privacy settings across platforms in Table 1 highlights that this default setting for *account suggestion* is in fact enabled on all platforms, not just Facebook.

With default privacy settings being more exposed than protective, previous research has measured unintended privacy leaks across various areas of the cyber world [13, 22, 31, 40–43, 60, 66, 71]. For example, Keküllüoglu et al. reported that 10% of 635K public tweets with the phrase "happy for you" exposed users' life events, ranging from marriage to surgery, and 8% of them directly revealed events associated with private accounts [35–37]. Similarly, Tandon et al. reported that 10.5% of 41 million public transaction records on Venmo contained sensitive information, as these transaction notes are publicly visible by default [63]. These results raise concerns about the extent of potential risks caused by default privacy settings [1–3, 5, 70]. Users who cannot locate or understand privacy settings provided by platforms are forced to settle for the default values, which are generally more exposed than they prefer [9, 21, 38].

2.3 Privacy Setting Locations

Given that default settings are usually more exposed than what users prefer, they need to manually adjust these settings in order to achieve their preferred privacy. Difficulties in locating these settings may result in users adjusting their privacy incorrectly or giving up on adjusting it altogether.

Ramokapane et al. conducted task-based interviews with mobile users, asking whether they were aware of manufacturer-provided privacy features such as ad identifiers or location services, and instructing them to locate these features [57]. They found that many users were unaware of these privacy features, and even when they were aware, they could not easily locate and adjust them. Chen et al. tasked mobile users to locate several privacy settings across hundreds of mobile applications and asked them to rate how difficult these settings were to locate [20]. They found that nearly 50% of these settings were difficult to locate. Frik et al. employed a direct questioning approach, asking users whether they were aware of a given mobile privacy setting and its default, and how difficult they thought it would be to locate the setting [25]. Similarly to other previous studies, they found that many users were not aware of mobile privacy settings and their defaults. In their study, over 60% of users believed that it will be easy for them to locate and configure the settings. However, our findings, which instructed users to actually locate the settings, show that nearly 80% of them found at least one setting hard to locate, highlighting a gap between expectation and reality.

2.4 Summary

The *novelty* of our work lies in (1) studying privacy settings across multiple platforms, (2) examining nine chosen, common privacy settings, and (3) simultaneously measuring awareness, preferences, and discoverability, which enables us to identify correlations among these three features. We summarize how our work is similar to and different from prior work using Table 2. First, we are not interested in mismatches between expected and actual privacy settings as they have been extensively studied [44–48]. Instead, we apply the direct questioning approach to measure user awareness and preferences regarding default privacy settings. As opposed to previous studies that only used text descriptions [7, 18, 25, 65], we provide screenshots of privacy settings and assess user awareness based on their ability to visually identify such settings (**awareness**). Having screenshots of settings helps reduce bias, as users who may not recognize settings from text descriptions or memory alone could provide inaccurate responses. We then display the default value for each privacy setting and ask users if they are satisfied with it or if they would prefer more or less privacy (**preferences**). Second, we apply the direct questioning approach to a range of privacy settings on a platform, as opposed to many previous studies that focused primarily on a single setting (e.g., audience, ads), except the recent work by Lowens et al. [45]. This expands our findings beyond just post or ad privacy, to include further perceptions of privacy settings relevant to everyday use, such as who can send messages to the user or who can see their friends list. Third, we directly measure users' ability to locate privacy settings, in addition to their awareness and preferences, as a way to evaluate the usability of these settings (**discoverability**). We choose the task-difficulty approach by Chen et al. [20], as described in Section 2.3 to determine if the settings are hard to locate. We only focus on six popular social media applications and a set of common privacy settings (Table 1), whereas Chen et al. studied many mobile applications, not limited to social media, and all privacy settings on those applications. Fourth, we study privacy settings across multiple platforms, as opposed to most previous work, which focused on a single platform, usually Facebook. Aljohani et al. presented high-level findings on information disclosure awareness (e.g., targeted ads) on social media, using multiple platforms as a way to to diversify the user population. We go beyond that in two ways: we study a wider range of privacy settings, and we leverage multi-platform analyses to gain deeper insights into cross-platform similarities and platform-specific differences (**differences**). Fifth, we simultaneously study awareness, preferences, and discoverability, enabling us to identify correlations among these three research questions, which have never been studied before (**correlations**). To the best of our knowledge, we believe that our work is the first study that comprehensively measure these several aspects of privacy settings across multiple social media platforms within a single study.

Table 2: Comparison of our work with previous studies.

Ref.	Foci	Platforms	Year	Privacy Settings	Method
Liu et al. [44]	awareness	Facebook	2011	audience	mismatch measurement
Madejski et al. [46, 47]	awareness	Facebook	2012		
Mondal et al. [48]	awareness	Facebook	2019		
Lowens et al. [45]	awareness preferences	Facebook	2025	multiple	
Tuunainen et al. [65]	awareness	Facebook	2009	ads	direct questioning
Aljohani et al. [7]	awareness	Facebook, Instagram, X (Twitter), Snapchat	2016		
Pew Research Center [18]	awareness preferences	Facebook	2019		
Ramokapane et al. [57]	awareness discoverability	Mobile	2019	multiple	task-based interview
Chen et al. [20]	discoverability	Mobile	2019		task-difficulty
Frik et al. [25]	awareness preferences discoverability	Mobile	2022		direct questioning
Our work	awareness preferences discoverability correlations differences	Facebook, Instagram, X, LinkedIn, TikTok, Snapchat	2025	multiple	direct questioning, task-difficulty

Table 3: Demographics of participant sample (n=541).

	Num. (%)						
	Facebook	Instagram	X	LinkedIn	TikTok	Snapchat	Total
Age							
18-24	13 (11%)	7 (11%)	7 (12%)	13 (11%)	10 (8%)	6 (10%)	56 (10%)
25-34	39 (32%)	17 (28%)	20 (33%)	37 (31%)	38 (32%)	16 (27%)	167 (31%)
35-44	9 (8%)	6 (10%)	3 (5%)	10 (8%)	12 (10%)	8 (13%)	48 (9%)
45-54	32 (27%)	19 (31%)	23 (38%)	41 (34%)	42 (35%)	22 (37%)	179 (33%)
55-64	19 (16%)	11 (18%)	6 (10%)	13 (11%)	10 (8%)	7 (12%)	66 (12%)
65-74	7 (6%)	1 (2%)	1 (2%)	6 (5%)	7 (6%)	1 (2%)	23 (4%)
75+	1 (1%)	0 (0%)	0 (0%)	0 (0%)	1 (1%)	0 (0%)	2 (0%)
Gender							
Male	54 (45%)	32 (52%)	41 (68%)	61 (51%)	47 (39%)	29 (48%)	264 (49%)
Female	64 (53%)	28 (46%)	19 (32%)	57 (47%)	71 (59%)	31 (52%)	270 (50%)
Non-binary	2 (2%)	1 (2%)	0 (0%)	2 (2%)	2 (2%)	0 (0%)	7 (1%)
Education							
<=High school	33 (28%)	16 (26%)	12 (20%)	20 (17%)	36 (30%)	16 (27%)	133 (24%)
Associate	6 (5%)	2 (3%)	6 (10%)	12 (10%)	9 (8%)	6 (10%)	41 (8%)
Bachelor	55 (46%)	29 (48%)	30 (50%)	65 (54%)	50 (42%)	22 (37%)	251 (46%)
Master	18 (15%)	10 (16%)	11 (18%)	19 (16%)	19 (16%)	14 (23%)	91 (17%)
Doctoral	2 (2%)	1 (2%)	0 (0%)	1 (1%)	4 (3%)	0 (0%)	8 (1%)
Professional	5 (4%)	3 (5%)	1 (2%)	3 (2%)	2 (2%)	1 (2%)	15 (3%)
Prefer not to say	1 (1%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (2%)	2 (0%)
Tech background							
Yes	33 (28%)	19 (31%)	20 (33%)	42 (35%)	38 (32%)	20 (33%)	172 (32%)
No	87 (72%)	42 (69%)	40 (67%)	78 (65%)	82 (68%)	40 (67%)	369 (68%)
Region							
Asia	0 (0%)	0 (0%)	2 (3%)	2 (2%)	3 (2%)	2 (3%)	9 (2%)
Africa	13 (11%)	8 (13%)	8 (13%)	30 (25%)	16 (13%)	6 (10%)	81 (15%)
North America	25 (21%)	19 (31%)	18 (30%)	38 (32%)	39 (32%)	20 (33%)	159 (29%)
South America	8 (7%)	1 (2%)	1 (2%)	7 (6%)	4 (3%)	2 (3%)	23 (4%)
Europe	69 (57%)	30 (49%)	30 (50%)	26 (22%)	47 (39%)	29 (48%)	231 (43%)
Australia	5 (4%)	3 (5%)	1 (2%)	11 (9%)	5 (4%)	0 (0%)	25 (5%)
Others	0 (0%)	0 (0%)	0 (0%)	6 (5%)	6 (5%)	1 (2%)	13 (2%)
Total	n=120	n=61	n=60	n=120	n=120	n=60	n=541

3 Methodology

We designed our survey to measure social media users' awareness of, preferences for, and ability to locate selected nine privacy settings. We focused on social media platforms including Facebook, Instagram, X, LinkedIn, TikTok, and Snapchat. We selected these platforms due to their popular usage [61]. Although LinkedIn is less popular than the rest, we included it, because its primary use modality (i.e., work and professional networking) differs from that of other platforms. For each platform, we selected a list of privacy settings based on previous work [20, 45]. Specifically, we focused on

privacy settings that are commonly available across platforms. Table 1 summarizes the privacy settings we selected. It shows whether the setting is available on which platform, its default option set by the platform, and the series of clicks needed to locate the setting, or what Chen et al. called *UI-path* [20]. Figure 4 in Appendix displays an example of a UI-path.

We piloted our survey with 10 members from our research group and collected initial feedback, which led to study revisions. We further piloted our study with 30 online participants to gather and address further feedback, before officially launching the study. Data collection took place from November 2024 to January 2025. We collected a total of 664 responses, eliminated incomplete or random responses, and retained 541 responses for data analysis.

3.1 Ethical Considerations

All participants were anonymous. Each participant was rewarded $3.00 for their participation. They were provided with informed consent (Appendix A) before beginning of the study, and the study was approved by our Institutional Review Board (IRB) as exempt.

3.2 Questionnaires

We designed our survey using Qualtrics (www.qualtrics.com), consisting of six questionnaires, one for each social media platform. Each questionnaire contains three different sections including: (a) user awareness and preferences for different privacy settings, (b) setting discoverability, and (c) demographics and platform usage.

Before starting the survey, participants were asked to provide informed consent (Appendix A) and were given an overview of each section, along with the estimated completion time of 15 to 20 minutes. We used neutral language when describing our study in the informed consent and when providing instructions in the survey, to mitigate any bias in responses. Each participant was asked about one platform they use, which itself was randomly selected from those platforms they reported using. We will refer to participants responding to the questionnaire about a platform, such as Facebook, as "Facebook participants".

Awareness and preferences. The first section of our questionnaire contains two types of questions: 1. awareness questions of the type *Have you ever seen the privacy setting Z?* and 2. preference questions of the type *Are you satisfied with the default option for privacy setting Z?*. A list of privacy settings in each questionnaire is based on what is available on each platform as shown in Table 1. For example, there are 8 privacy settings in the Facebook questionnaire or 16 questions asked, whereas there are 5 privacy settings on Instagram, and 10 questions regarding those.

For each awareness question, we provided a screenshot to show the specific privacy setting to a participant, ensuring that they understand exactly which setting we refer to (Appendix B.1). For each preference question, we informed the participants which default option is set by the platform, and asked if they are satisfied with the default option or prefer it to be more or less private (Appendix B.2).

Discoverability. The second section begins with instructions for participants to locate the privacy settings, then confirm whether they can find them, and rate how difficult that was. Since this section requires sustained focus from participants, we ensured that each questionnaire only asks a participant to locate a small number of privacy settings. For platforms with five or fewer settings, we asked participants to evaluate each setting. For platforms with more than five privacy settings, we divided the questions in this section into two balanced sets and each participant was asked to discover settings from one of the sets. For example, Facebook has eight privacy settings, which we divided into two sets of four questions each. Each Facebook participant was shown four discoverability questions. We balanced a number of participants across question sets. As another example, Instagram has five privacy settings, so there is only one set of questions shown to all Instagram participants.

For each privacy setting, we asked participants to spend approximately two minutes trying to locate it. If they could not find the setting within that time, we asked that they select "unable to locate" on the questionnaire. Otherwise, they would be asked to rate how hard it was to locate the setting on a 5-point Likert scale, ranging from *very difficult* to *very easy*. We also included an optional text-response question, where participants could provide a UI path (Figure 4) that they took to the privacy setting. We used this voluntary text answer to estimate the reliability of participants' labels when they claimed that they successfully located the privacy setting (Section 3.4). Additionally, we embedded a timer using Qualtrics' timing feature [54]. This timer measured in the background how long a participant spent on each page. We then leveraged this information as one of the criteria to verify data quality of the responses (Section 3.4). We provided an example of how we ask participants to locate a privacy setting in the discoverability section, in Appendix B.3.

Demographic and usage. The last section contains general demographic questions, including age, gender, education, whether the participant has a technical background, and the region they currently reside in. We also asked which mobile operating system the participant used to locate privacy settings in the discoverability section, along with questions about general platform usage, such as the number of years they used the platform, frequency of usage, frequency of posting or sharing, and the number of other platforms the participant used. In this section, we also included an attention check to ensure data quality (Section 3.4). We employed a commitment request, asking participants to confirm that they had provided thoughtful answers to the survey (Appendix B.4). Previous work suggested that this type of check is more effective than other standard attention checks, such as factual checks (e.g., Which of these is a vegetable?) or textual attention checks (e.g., Please enter the word "Purple" in the box below) [26, 28].

3.3 Recruitment

We recruited 664 participants for our survey using *Prolific*, an online study platform (www.prolific.com). Each participant is allowed to complete the survey once, meaning that they will complete one questionnaire for the platform they used and were assigned to. As we collected responses, we performed quality checks on each (see Section 3.4), removed low-quality responses and recruited more participants, until we had the desired number per platform.

We initially planned to collect 60 responses per platform, and to balance them across younger and older groups (30 responses per group). With 30 samples per group (younger vs older), we have

80% statistical power to detect a medium-to-large effect size or difference between the two groups (Cohen's d ≈ 0.65).

Some platforms have many privacy settings. To make the study duration manageable for participants, we broke these platforms' questionnaires into two parts, each containing only half of the settings (Section 3.2). We recruited 120 participants with balanced samples of younger and older participants for those platforms (Facebook, LinkedIn and TikTok) to ensure that we had 30 older and 30 younger participants attempt to locate each privacy setting [1]. Table 3 summarizes our 541 participants' demographics.

We intentionally employed Prolific's screening to ensure that we have even distribution between participants based on age (younger: 18-44 years vs older: 45+ years old) and gender (male vs female). Our participants skew towards higher education (>= Bachelor) (67%) and no technical background (68%). Majority of our participants are from Europe (43%), followed by North America (29%) and Africa (15%). To ensure data quality, we only recruited participants who were fluent in English, have made 200 or more submissions and had higher than 97% approval rate. The survey took an average of 17 minutes 35 seconds to complete (median: 15 minutes 54 seconds) and participants were rewarded $3.00 for their participation.

3.4 Data Quality

To ensure data quality, we continuously reviewed responses from the participants and adjusted our screening questions to achieve balanced responses across platforms and age groups. We rejected all responses from a participant that failed the attention check or that spent less than expected time to locate any given privacy setting. We calculated the expected time per setting as $\mu - (1.5 \times sd)$ where μ is the measured mean time for all participants to locate the given privacy setting on the given platform and sd is the corresponding standard deviation. For example, Instagram participants took an average of 101 seconds ($sd = 54.62$) to locate the *audience* privacy setting. We removed all responses from participants that spent less than $101 - (1.5 \times 54.62) = 19$ seconds to locate the *audience* setting. Additionally, we found a few responses with write-in text answers that appeared AI-generated and rejected those responses. Overall, we removed 123 out of 664 participants' responses and kept 541 participants' responses for data analysis.

To verify the reliability of participants' labels when they claimed that they found the privacy setting, we manually reviewed the UI-path answers (Figure 4) provided by volunteer participants (Section 3.2). We used two sets of ground truth for UI-paths, one for iOS and another for Android, to account for differences in UI-paths on participants' devices. Out of 541 participants, 325 of them (61%) volunteered to provide text answers. Across a total of 1,296 text answers [2], 59 of them (4%) were incorrectly labeled, i.e., the participant claimed that they found the given privacy setting, but their text answer revealed that they found a different setting. This small fraction of mislabeling suggests that participants likely provided truthful answers to discoverability questions. We discuss further limitations of our study in Section 3.6.

3.5 Data Analysis

For RQ1–RQ3 (awareness, preferences, and discoverability), we report descriptive statistics and present comparisons between different privacy settings and platforms. Specifically, we used the Complementary Cumulative Distribution Function (CCDF) to display the relationship between the fraction of users and the number of privacy settings they have never seen (RQ1), prefer to be more private (RQ2), and feel are hard to locate (RQ3). For each privacy setting, we also calculated these fractions for each platform to highlight any differences among them.

For RQ5 (differences), we conducted several single regression analyses to investigate differences among participants from different demographic groups, usage patterns, or across different platforms. Specifically, we defined 3 continuous dependent variables including a percentage of privacy settings a user has seen (*P_SEEN*), a percentage of privacy settings a user prefers to be more private (*P_PRIVATE*), and a percentage of privacy settings a user feels are hard to locate (*P_HARD*). Since each platform has a different number of privacy settings, we use percentages instead of counts of privacy settings in RQ1–RQ3.

We also defined an additional continuous dependent variable, which is the average number of seconds a participant spent locating a privacy setting (*A_TIME*). This value is derived from the time data, which is collected in the discoverability section of the questionnaire (Section 3.2) and represents the average time participants spent to locate *any* privacy setting on the given platform. We ran bivariate Pearson correlations among *P_SEEN*, *P_PRIVATE*, *P_HARD*, and *A_TIME* to determine any relationships among awareness, preferences and discoverability for RQ4 (correlations).

We defined 10 independent variables: age (younger: 18-44 vs older: 45+), gender (Female vs Male), education (Bachelor and higher vs High school and lower), whether a user has a technical background (No vs Yes), a number of years a user has been using the platform (3+ vs Less than 3), usage frequency (Daily vs Weekly vs Less frequent than weekly), post and sharing frequency (Once or more per month vs Less than once a month), mobile operating system (OS) used for locating privacy settings (Android vs iOS), a number of different platforms a user uses (continuous), and platform (Facebook, Instagram, X, LinkedIn, TikTok and Snapchat). We did not include non-binary gender (Table 3) and "Other OS" (Table 5) in the regression analyses, because each only represented 1% of all responses. We applied dummy coding to all categorical independent variables with the most frequent value as the reference (i.e., the first value in the parentheses). For the categorical independent variable "platform", we rotated the reference to ensure that we compared every possible pair of platforms. We ran a single linear regression model, specifically an ordinary least squares model (OLS), between each independent variable and each continuous dependent variable.

Since we ran multiple tests on each dependent variable for RQ5, we addressed the multiple comparisons problem by applying the Bonferroni correction [8]. Specifically, we denote 0.05 as the default significant threshold and (0.05 / number of tests per dependent variable) as the corrected threshold of significance. We ran a test

[1] Instagram ended up having 61 participants

[2] The total number of text answers is a sum across platforms of products of number of text answers per platform questionnaire and the number of volunteer participants who provided text answers for that platform. For example, Facebook has 4 text answers per questionnaire, and there are 70 participants that provided text answers. Hence, the total number of text answers for Facebook is 280.

once for each of nine independent variables. For the platform variable, we rotated the reference five times in order to compare every possible pair of platforms, thus we ran five tests. In total, we ran 14 tests per dependent variable. As a result, the corrected threshold of significance becomes 0.0036.

3.6 Limitations

Our study has limitations inherent to the nature of online surveys. Participants' self-reported responses may not always be accurate, especially in the discoverability section, where users reported whether they were able to locate the privacy settings. There are two types of errors that can occur in this section. First, participants may provide false positive answers, claiming they found the settings when, in reality, they did not or they found wrong settings. We used the voluntary answers to UI-path questions to identify some false positives, as described in Section 3.4, where a participant located a different setting than the one we asked them to find. We corrected these participant responses, converting them from positive to "This setting is hard to locate" (i.e., "very difficult" or "difficult" on the Likert scale). There still may be some false positives in the responses, which we cannot identify. Thus, our reported findings should be regarded as a lower bound on the actual number of users who were unable to locate a given privacy setting.

Second, participants may provide false negative answers, claiming they were unable to locate the privacy settings when, in reality, they had found the setting, but did not realize it. In some cases, we could ascertain that this has happened, because the participant provided the voluntary response to the UI-path question, and that response indicated the correct path. Even so, we retained the participants' initial (negative) answers, because their doubts about whether they have located the privacy setting suggest that they may struggle to effectively use the setting for their intended purpose.

In the awareness section, participants answered questions about whether they have seen a privacy setting from memory, which may produce unreliable answers. Through multiple rounds of pilot studies, we found that providing a snapshot of the privacy setting helped participants provide more accurate answers. Thus, we included the snapshots to reduce the possibility of inaccurate responses.

Our participants were located mostly in Europe and North America. Results from different regions (or distributions) may differ. Further, we selected a set of privacy settings for the questionnaires based on previous work [20, 45]. Because our set does not include all privacy settings on any given platform, our findings may not apply to settings we did not include in the study.

4 Results

We present our findings in this section, following the order of research questions.

4.1 Awareness (RQ1)

We report the number of privacy settings each participant has never seen. Across the six platforms, 80% of participants have never seen at least one privacy setting and 58% have never seen multiple. We present the breakdown for each platform in Figure 1. Instagram has the highest fraction, 93% of participants have never seen at least one setting, and 66% have never seen multiple. LinkedIn ranks second, where 90% have never seen at least one setting, and 72% have never seen multiple, while Facebook follows in third, 84% have never seen at least one, and 62% have never seen multiple. These fractions suggest that even though these settings are prevalent and commonly available across platforms, a considerable number of users are still not fully aware of their existence.

We also report the fraction of participants who have never seen a given privacy setting in Table 4. Most privacy settings are familiar to majority of users, but there are a few that are more obscure. For example, 82% of Instagram participants and 70% of X participants have never seen the *video* setting. With short video content gaining worldwide recognition in 2018 on TikTok [29], Instagram introduced its own version of short video content, called "Reels" in 2020 [32]. The "video" setting on Instagram refers to whether others can download users' Reels on the platform. Given the relatively recent introduction of this feature, it is understandable that many Instagram users are unaware of its related privacy setting. Similarly, X recently (2023) introduced its *video* setting to allow users to control whether others can download their video posts [52], thus 70% of users are still unaware of the setting. Additionally, 67% of LinkedIn participants and 54% of Instagram participants have never seen the *ads* setting. These results are consistent with a previous Pew Research survey, which reported that 74% of Facebook users are unaware of the *ads* setting in 2019 [18]. Our study shows that in 2024, 41% of Facebook users were still unaware of the setting, and users of Instagram (54%), LinkedIn (67%) and TikTok (46%) were similarly unaware of the *ads* setting. Some other examples of privacy settings that are not familiar to users on specific platforms are as follows. 46-56% of Facebook, X and LinkedIn participants have never seen the *account suggestion* settings, compared to 23–25% of TikTok and Snapchat participants. 58% of Facebook participants have never seen the *search engine* setting, compared to 38% of LinkedIn participants. These platform-specific differences in awareness suggest that the way platforms organize their privacy settings greatly impacts user familiarity with them and, consequently, users' ability to adjust them to fit their needs.

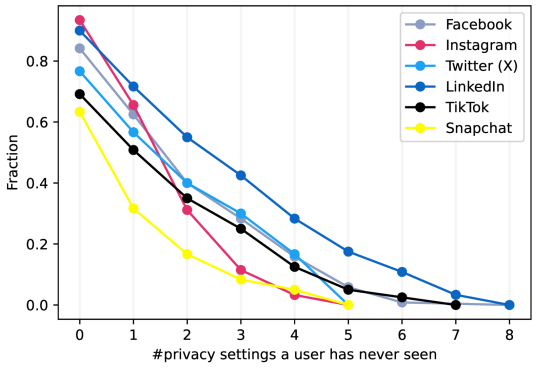


Figure 1: CCDF of the number of privacy settings a participant has never seen.

Table 4: The fraction of participants on each platform (n=60) who have *never seen* a privacy setting, prefer the default to be *more private*, and feel the setting is *hard to locate* for each privacy setting (highlighted cells are the fractions of 50% or more).

Privacy Settings	%	Facebook	Instagram	X	LinkedIn	TikTok	Snapchat
audience	*never seen*	2.50%	9.84%	40.00%	16.67%	12.50%	10.00%
	more private	18.33%	55.74%	30.00%	11.67%	42.50%	31.67%
	hard to locate	31.67%	6.56%	65.00%	55.00%	15.00%	20.00%
message	*never seen*	30.00%	16.39%	28.33%	32.50%	20.00%	18.33%
	more private	50.83%	57.38%	11.67%	25.00%	10.00%	50.00%
	hard to locate	36.67%	8.20%	15.00%	25.00%	16.67%	6.67%
ads	*never seen*	40.83%	54.10%	35.00%	66.67%	45.83%	36.67%
	more private	80.00%	63.93%	73.33%	70.00%	61.67%	68.33%
	hard to locate	73.33%	77.05%	35.00%	58.33%	33.33%	38.33%
activity status	*never seen*	22.50%	42.62%	-	39.17%	32.50%	35.00%
	more private	60.83%	59.02%	-	46.67%	52.50%	51.67%
	hard to locate	31.67%	63.93%	-	28.33%	38.33%	23.33%
account suggestion	*never seen*	55.83%	-	46.67%	45.83%	22.50%	25.00%
	more private	68.33%	-	70.00%	40.00%	70.00%	63.33%
	hard to locate	43.33%	-	43.33%	58.33%	26.67%	55.00%
connection view	*never seen*	15.83%	-	-	46.67%	24.17%	-
	more private	70.00%	-	-	43.33%	60.83%	-
	hard to locate	43.33%	-	-	15.00%	20.00%	-
video	*never seen*	-	81.97%	70.00%	-	42.50%	-
	more private	-	67.21%	60.00%	-	71.67%	-
	hard to locate	-	65.57%	50.00%	-	26.67%	-
profile view	*never seen*	13.33%	-	-	33.33%	-	-
	more private	80.83%	-	-	36.67%	-	-
	hard to locate	36.67%	-	-	55.00%	-	-
search engine	*never seen*	57.50%	-	-	38.33%	-	-
	more private	70.83%	-	-	38.33%	-	-
	hard to locate	48.33%	-	-	75.00%	-	-

4.2 Preferences (RQ2)

We report on those privacy settings, where participants prefer a more private default option. Across the six platforms, 92% of participants prefer at least one default setting to be more private and 83% prefer multiple to be more private. We present the breakdown for each platform in Figure 2. Every platform has a very high fraction of participants who prefer at least one default setting to be more private: 95% for Instagram, 93% for Facebook, LinkedIn, and TikTok, 92% for X, and 88% for Snapchat. The fractions of participants who prefer multiple default settings to be more private are also high: 91% for Facebook, 87% for Instagram, 86% for TikTok, 80% for X, 77% for LinkedIn, and 75% for Snapchat. These results suggest that platforms' default settings are generally more exposed than what users prefer, which aligns with previous findings for Facebook user preferences [44, 45]. Our results complement previous research, by highlighting an industry-wide misalignment between user preferences and the default privacy options set by platforms.

We present the fraction of participants who prefer more private default for each privacy setting on each platform in Table 4. We summarized key findings per privacy setting using the reference defaults in Table 1:

audience: Most participants are satisfied with the default setting when set to "Friends" or just people they know: only 32% of Snapchat, 18% of Facebook and 12% of LinkedIn participants prefer the more private default. However, when the default setting is more exposed (e.g., "Public" account), the fraction of participants who favor the more private default increases: 56% for Instagram, 42% for TikTok and 30% for X.

message: Participants prefer a more private setting when the default setting is more exposed than "Friends". With the default being "Anyone can message you", 57% of Instagram, 51% of Facebook and 50% of Snapchat participants favor the more private default. LinkedIn is an exception here. Even though the default is also

"Anyone", due to fact that the platform is used for professional networking, most participants are satisfied with the current default (only 25% favor the more private setting).

ads: Participants across all platforms consistently prefer the default setting to be more private (i.e., not using your information for personalized ads), with Facebook standing out at 80%, while the others range between 62% (TikTok) and 73% (X) of participants. This aligns with the previous finding from the Pew Research Center, which reported that 51% of Facebook users are uncomfortable with the platform's default practice of creating a list of their interests and traits for personalized ads [18]. Our result further emphasizes that this discomfort is prevalent across different platforms.

activity status: Participants prefer the default setting to be more private (i.e., not allowing others to see when you are online), with Facebook and Instagram standing out at 61% and 59%, respectively, while the others range between 47% (LinkedIn) and 53% (TikTok) of participants. Overall, around half of users prefer not to let others see when they are active on social media. This preference may be due to the rise in cyberstalking, with 30–40% of stalking victims reporting that their activities were monitored through social media [49].

account suggestion: Participants prefer the default setting to be more private (i.e., not suggesting your account to others via phone number or email), with 63% (Snapchat) to 70% (X and TikTok) of participants favoring more private option than the default. LinkedIn has a lower fraction than the rest (40%), which is understandable given its focus on professional networking.

connection view: When a default is set to "anyone", participants prefer a more private setting. This is the case for 70% of Facebook and 61% of TikTok users. This result suggests that users prefer their network information to be visible only to their own network, in contrast to the social media business model, which benefits from higher exposure of user networks. Oversharing such information can lead to harm, for example when Joe Biden's Venmo account was exposed in 2021 due to public visibility of his friend list [27].

video: Participants across different platforms consistently prefer the default setting to be more private (i.e., not allowing people to download your videos), with 72% of TikTok, 67% of Instagram, and 60% of X participants favoring the more private default. Moreover, many users are unaware of the setting (Section 4.1), which indicates that users' videos are generally more exposed that they desire, without their knowledge or consent.

profile view: Participants' preferences depend on the platform. When the default setting is "Anyone can view your profile details" (e.g., education, location), 81% of Facebook participants favor a more private setting, while on LinkedIn only 37% favor a more private setting. This suggests again that participants are satisfied with being more exposed on LinkedIn than elsewhere, due to LinkedIn's professional networking nature.

search engine: Similar to *profile view*, 71% of Facebook participants prefer a more private default setting than "Search engine can find your profile", while on LinkedIn only 37% of participants prefer a more private default setting.

4.3 Discoverability (RQ3)

We report the number of privacy settings each participant feels are hard to locate. We determined that a given setting was hard to locate when participants either could not find it or rated finding this setting as "*difficult*" or "*very difficult*" (Section 3.2). Across the six platforms, 79% of participants feel that at least one privacy setting is hard to locate, and 50% feel that multiple are hard to locate. We present the breakdown for each platform in Figure 3. 90% of Instagram, 89% of LinkedIn, 88% of X, 82% of Snapchat and 80% of Facebook participants feel that at least one privacy setting is hard to locate. TikTok, however, has a smaller fraction of 55%. This may be because the UI-paths for TikTok's privacy settings are more straightforward, and each click contains clearer and more concise keywords compared to other platforms. We discuss this further in Section 5.2.2. For the fraction of participants who feel multiple privacy settings are hard to locate, Instagram ranks first with 79%, while TikTok and Snapchat have much lower percentages at 23% and 38%, respectively. The other platforms fall between 55% (Facebook) and 60% (LinkedIn). These fractions suggested that privacy settings in general are difficult to locate.

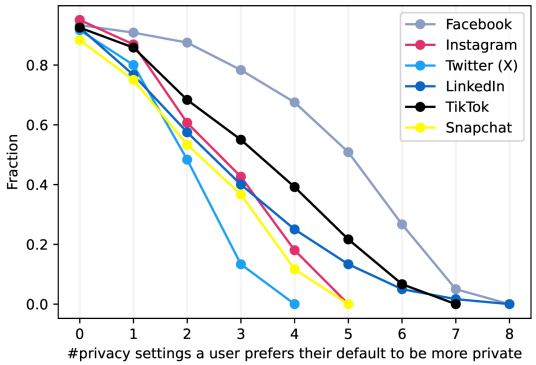


Figure 2: CCDF of the number of privacy settings a participant prefers their default to be more private.

For each privacy setting on each platform, we also report the fraction of participants who feel this setting is hard to locate in Table 4. When this fraction exceeds 50%, we say that this setting is hard to locate. Participants face varying difficulties in locating privacy settings across different platforms. We summarized key findings per platform using the reference UI-path in Table 1:

Facebook: 1 out of 8 privacy settings is considered hard to locate, with highest being the *ads* setting (rated "hard to locate" by 73% of participants). One possible reason could be that the *ads* setting takes 5 clicks to locate, while other settings takes 3-4 clicks.

Instagram: 3 out of 5 privacy settings are considered hard to locate. Specifically participants feel the *ads* (77%), *video* (66%), and *activity status* (64%) settings are hard to locate. This may be because 43-82% of users are unaware of these setting (Section 4.1).

X: 2 out of 5 privacy settings are considered hard to locate. Specifically, participants feel the *audience* (65%) and *video* (50%) settings are hard to locate. This may be because many users are unaware of the *video* setting (Section 4.1) and X uses vague wording to describe each click on the UI-path to the *audience* setting (Section 5.2).

LinkedIn: 5 out of 8 privacy settings are considered hard to locate. Specifically, participants feel the *search engine* (75%), *ads* (58%),

account suggestion (58%), *audience* (55%) and *profile view* (55%) settings are hard to locate. Given the platform's focus on professional networking, it is understandable that LinkedIn users may not be highly concerned about their privacy (supported by our results in Section 4.2). As a result, they may not adjust their privacy settings beyond the defaults, which could explain why users (though aware of the settings) are not familiar with how to locate them.

TikTok: None of the privacy settings are considered hard to locate, as all fractions are below 50%. This is not surprising, given that all TikTok UI-paths are clear and precise (Section 5.2).

Snapchat: 1 out of 5 privacy settings are considered hard to locate, with 55% of participants feeling the *account suggestion* setting is hard to locate. Again, this could be explained by the one additional click required to locate the *account suggestion* setting (4 clicks), compared to other settings (3 clicks).

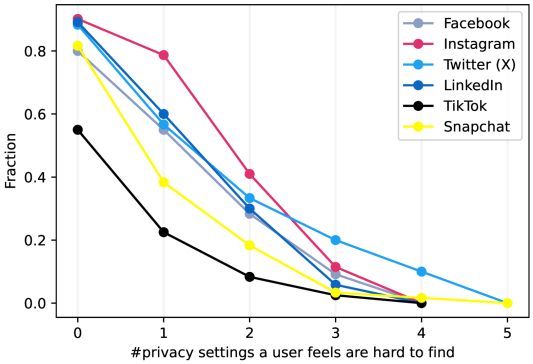


Figure 3: CCDF of the number of privacy settings a participant feels are hard to locate.

4.4 Correlations (RQ4)

We ran bivariate Pearson correlations on responses from all platforms among *P_SEEN*, *P_PRIVATE*, *P_HARD*, and *A_TIME*. We use 0.05 as the significance threshold in this subsection. We found that *P_HARD* is significantly positively correlated with *A_TIME*, meaning that the harder users perceived locating privacy settings, the more time they actually spent locating them (r(N=541) = 0.162, p < 0.001). Given this positive correlation, we will only use *P_HARD* to represent the difficulties users face in locating privacy settings for the remainder of this subsection.

We found that *P_SEEN* is significantly negatively correlated with *P_HARD*, meaning that the fewer privacy settings users have seen, the harder for them to locate those settings (r(N=541) = -0.328, p < 0.0001). This counters the assumption made by platforms that simply offering privacy settings is sufficient to protect user privacy. If users are unaware of these settings, they are likely to face difficulties in adjusting them (once made aware), which may result in incorrect adjustments or giving up on making changes altogether. We also found that *P_PRIVATE* is significantly positively correlated with *P_HARD*, meaning that users who prefer more privacy face more difficulties in locating the correct settings (r(N=541) = 0.089, p = 0.038). The last finding is very important, because it suggests that users who experience difficulties in locating privacy settings are the ones who desire more privacy, emphasizing the need for a straightforward process to adjust privacy settings for these users.

We also ran the same correlation analysis on responses from each platform. We found that *P_SEEN* is significantly negatively correlated with *P_HARD* on every platform except TikTok (-0.512 ≤ r ≤ -0.235, p ≤ 0.015). This suggests that TikTok users do not find their privacy settings difficult to locate, even if they had never seen them before and were learning about them for the first time during the study. In fact, we discuss next in Section 4.6 that TikTok users actually find their privacy settings significantly easier to locate compared to users of other platforms. This indicates that good platform design can address discoverability issues.

4.5 Demographic and Usage Differences (RQ5)

We show the demographic distribution of our participants in Table 3. There was 1% of participants who identified as non-binary. We have compensated them for their participation, but we did not use their responses in statistical analysis, due to small sample size. Most participants have been using their chosen platform for more than 3 years, except for TikTok, which is the most recent platform (Figure 5). Most participants use the platform weekly or more often (Figure 6), while rarely posting or sharing on the platform (Figure 7). 62% of participants use Android and 37% use iOS to locate privacy settings in Section 4.3 (Table 5). There was less than 1% of participants who used other operating systems. We removed these responses, since there were too few samples for statistical analysis. We also show the distribution of the number of platforms a participant uses, with most using 3-5 platforms (Figure 8).

As described in Section 3.5, we ran a linear regression model between each independent variable and each continuous dependent variable (*P_SEEN*, *P_PRIVATE*, *P_HARD*, *A_TIME*). Table 6 shows cases where differences exist between demographic groups or usage patterns – differences where p-values are lower than the corrected threshold of significance are highlighted in bold.

age: Older users (45+) have, on average, seen 10% fewer privacy settings than younger users (18 − 44) (*P_SEEN*: β^{45+}_{18-44} = -0.101, p^{***} < 0.0001). Given their lower engagement with online technologies [19], it is expected that older users are less aware of privacy settings than younger users.

gender: Female users prefer, on average, higher-than-default privacy for 8% more of the settings, compared to male users (*P_PRIVATE*: β^{Male}_{Female} = -0.079, p^{***} = 0.001). This aligns with previous surveys by Pew Research Center [15] and Forbes [10], which indicated that women are more likely to restrict their social media profiles compared to men.

usage freq: Users who use the given platform less frequently (i.e., less often than weekly) find, on average, 7% more of their privacy settings hard to locate compared to those who use the platform daily (*P_HARD*: $\beta^{<Weekly}_{Daily}$ = 0.069, p^{***} = 0.002). This is expected, as more frequent interactions with the platform lead to higher familiarity and easier navigation. In this analysis, we did not see a significant difference in privacy setting discoverability or familiarity between users who use the platform daily versus weekly.

post freq: Users who post or share less frequently prefer, on average, higher-than-default privacy on 9% more of their settings, compared to those who post or share more frequently (*P_PRIVATE*: $\beta^{>=Monthly}_{<Monthly}$ = -0.090, $p^{***} < 0.001$). This aligns with previous findings that show users who prioritize their privacy online may choose to be more selective about the information they share, which can result in less frequent posting [16, 17, 33].

os: iOS users, on average, spend 16 seconds less to locate privacy settings than Android users (*A_TIME*: $\beta^{Android}_{iOS}$ = -15.830, p^{**} = 0.004). Statistically, this is not a significant difference ($p > 0.0036$), but we mention it, since the p-value is very close to the threshold. This result supports the notion that Android typically offers more customizations, while iOS prioritizes ease of use.

#platforms: Users who use more platforms have seen more privacy settings compared to those who use fewer platforms (*P_SEEN*: β = 0.029, p^{***} = 0.001). This supports the idea that the more users use social media, the greater their familiarity with privacy settings. Additionally, users who use fewer platforms would restrict more of their privacy settings compared to users who use more platforms (*P_PRIVATE*: β = -0.033, $p^{***} < 0.001$). Thus, lower exposure to social media leads to higher sensitivity around privacy choices.

4.6 Platform-specific Differences (RQ5)

We ran linear regression models to test for differences across *platforms*. We found that the differences exist and their effect sizes are generally larger comparing to those for demographic and usage independent variables. Table 7 shows cases where differences exist between platforms – differences that pass the corrected threshold of significance are highlighted in bold. We also discuss cases where p-values are close to the significance threshold (e.g., 0.004 or 0.005).

P_SEEN: Facebook users have, on average, seen 10-14% more privacy settings compared to users of other platforms ($0.101 \leq |\beta| \leq 0.142$, $p^{**} \leq 0.004$), while Instagram, X, and LinkedIn users have, on average, seen 10-19% fewer privacy settings compared to users of other platforms ($0.101 \leq |\beta| \leq 0.190$, $p^{**} \leq 0.004$). Facebook has been around longer and offers a set of privacy settings that have stayed consistent over time. In contrast, as we discussed in Section 4.1, Instagram and X have recently introduced the *video* setting, which many users are unaware of. This likely contributes to the overall lower awareness of privacy settings on these platforms. For LinkedIn, users may be less interested in restricting their privacy settings, because that would diminish the size of their professional network, and contradict their goals for using the LinkedIn platform. This lower interest likely explains lower user familiarity with the platform's privacy settings.

P_PRIVATE: Facebook users prefer, on average, higher-than-default privacy on 10-24% more settings, compared to users of other platforms ($0.098 \leq |\beta| \leq 0.235$, $p^{**} \leq 0.005$), while LinkedIn users prefer higher-than-default privacy on 14-24% fewer settings, compared to users of other platforms ($0.140 \leq |\beta| \leq 0.235$, $p^{***} \leq 0.001$). Given Facebook's history of privacy-related incidents, it is understandable that users may be more cautious about their privacy compared to those on other platforms. For LinkedIn, as discussed previously, users generally prioritize networking on the platform and are therefore more comfortable with lower privacy restrictions.

P_HARD: TikTok users find, on average, 9-32% fewer of their privacy settings hard to locate compared to users of other platforms ($0.089 \leq |\beta| \leq 0.316$, $p^{***} \leq 0.001$), while Instagram and X users find, on average, 13-32% more of their privacy settings hard to locate compared to users of other platforms ($0.130 \leq |\beta| \leq 0.316$, $p^{***} \leq 0.001$). We provide our observation and explanation behind these differences in Section 5.2.2.

A_TIME: Facebook users spend, on average, 35-39 seconds more to locate privacy settings compared to users of other platforms ($34.606 \leq |\beta| \leq 38.701$, $p^{***} \leq 0.0001$), while TikTok and Snapchat users spend, on average, 33-39 seconds less to locate privacy settings compared to users of other platforms ($33.036 \leq |\beta| \leq 38.701$, $p^{***} \leq 0.0001$). Since Facebook has been around the longest, it has inherently introduced more complexity over time due to the wide range of features developed throughout the years. As a result, it is understandable that users may require more time to navigate Facebook's settings compared to more recent platforms, like TikTok or Snapchat. To illustrate, we provide comparison screenshots between Facebook's post setting and Snapchat's story setting in Figure 9 and 10 in Appendix, respectively. We can see that, within the same click that users take to adjust the *audience* setting, Facebook contains more complicated settings than Snapchat, leading to more time needed to navigate Facebook's settings.

Summary. We found multiple significant differences across *platforms*, and their effect sizes are generally larger compared to those of demographic and usage factors. Notably, LinkedIn users are more comfortable with exposure compared to users of other platforms, and TikTok users find their privacy settings easier to locate compared to users of other platforms. We also ran linear regression models to test for differences across *platforms*, and how they might depend on the *age* factor. We report our finding in Appendix B.5. In short, we found that differences across *platforms* are moderated by the *age* factor. For example, among older participants, X users have seen fewer privacy settings and find them harder to locate compared to users of other platforms.

5 Discussion

We summarize our key findings compared to previous studies in Table 2, discuss them and provide recommendations for platforms.

5.1 Main Contributions

awareness. Our results reaffirm previous findings, and extend them beyond a single privacy setting or single platform. Previous work has shown that social media users were not generally aware of the *ads* settings. Tuunainen et al. reported that 73% of Facebook users were unaware that Facebook shared their information with third parties outside the platform in 2009 [65]. 10 years later, in 2019, Pew Research Center reported that a similar proportion of users (74%) remained unaware of targeted ads on Facebook [18], while in 2016, Aljohani et al. found that across Facebook, Instagram, X (Twitter at that time), and Snapchat, 66% of users were unaware of targeted ads on their platforms [7].

Our results show that in 2024, a relatively large proportion of Facebook users (41%) is unaware of the *ads* setting used for adjusting target ads privacy. This unawareness of the *ads* setting is also prevalent across Instagram, X, LinkedIn, TikTok and Snapchat,

with 35-67% of users on each platform being unaware. We also found that other privacy settings, such as *video*, are unfamiliar to 43–82% of users on Instagram, X, and TikTok. Our results confirm that some common privacy settings are unfamiliar to many users, regardless of the platform. Other settings may be more familiar to users on some platforms, yet unfamiliar on other platforms.

preferences. Our results reaffirm previous findings and extend them beyond a single platform. Lowens et al. reported that Facebook users generally preferred their default privacy settings to be more private [45]. Our results not only confirm the findings by Lowens et al., but more importantly, reveal an industry-wide misalignment in default privacy settings, where platforms prioritize user engagement over protection, while users prefer protection [11]. The exception is LinkedIn, where only the *ads* setting is preferred by the majority of users (70%) to have more private defaults, consistent with other platforms (62-80%). For other privacy settings, LinkedIn users are satisfied with the default settings, suggesting that they prioritize engagement (i.e., networking) over privacy on this platform, as opposed to other platforms.

discoverability. Our results reaffirm previous findings, with the specific focus on social media applications and their privacy settings. Chen et al. reported that nearly 50% of mobile applications' privacy settings were difficult to locate [20]. In support, we found that 79% of participants feel that at least one setting on their social media platform is hard to locate. Our results also counter the findings by Frik et al., who reported that over 60% of users believed that they could easily locate privacy settings [25]. This highlights a common misconception among users that adjusting privacy settings is easy, whereas in reality, they struggle more than they expected.

correlations. Our results show, for the first time, correlations among awareness, preferences, and discoverability. No previous studies have simultaneously explored these three research questions within a single study. We found that the fewer privacy settings users have seen, the harder for them to locate the settings. This applies to all platforms except TikTok, highlighting that good user interface design can help address the discoverability issues. We also found that users who desire more privacy are the ones who find it more difficult to locate privacy settings, further emphasizing that user preferences are ill-aligned with the default privacy and that users cannot easily close this gap through their own actions.

differences. Our results reaffirm previous findings and add cross-platform analysis. We found that older users struggle more with privacy settings than younger users. They have seen fewer settings and spend more time locating them–consistent with Lowens et al. [45]. Our cross-platform analysis reveals further insights, including that users find privacy settings on TikTok the easiest to locate compared to other platforms.

5.2 Recommendations and Future Research

In this section, we discuss implications of our findings and provide recommendations for platforms.

5.2.1 User Preferences Towards Default Privacy Settings.

We observe that users are generally satisfied with the default settings when these are set to "Friends". For example, the default of *audience* for Facebook and LinkedIn is set to "Friends" (Table 1) and less than 20% of participants from both platforms prefer it to be more private (Table 4), while 80% are satisfied with the default.

One exception is LinkedIn where users prefer higher exposure (e.g., 60% are satisfied with everyone being able to see their profile). LinkedIn is primarily used for professional networking and its users may benefit from higher exposure. This suggests that the purpose of a platform matters when determining the exposure level of the default settings [67].

Recommendations. We recommend that platforms employ a default setting of "Friends" for user profile, posts and any other data shared by users on the platform. It is crucial for them to prioritize user privacy by setting a safer default, while allowing users to increase their exposure if they so desire [69]. We believe that a middle ground exists, where platforms can adjust the exposure level of default privacy settings to help protect user privacy, while maintaining their social media business model.

5.2.2 Difficulties in Locating Privacy Settings.

We observe that users generally find the privacy settings difficult to locate when their series of clicks (i.e., UI-path in Figure 4) are not straightforward. For example, we notice that 65% of X users and 55% of LinkedIn users find the *audience* settings hard to locate, which is higher than on other platforms (Table 4). When we examined the UI-paths of *audience* for these two platforms (Table 1), we identified two design flaws that cause these difficulties:

First, the UI-path for X to *audience* (`Profile > Settings and privacy > Privacy and safety > Audience and tagging > Protect your posts`) does not use clear wording to properly describe the setting users are trying to adjust (in this case, switching their profile between public and private). Conversely, Instagram and TikTok have more straightforward UI-paths and they use specific wording to describe the intended effect of the settings (Instagram: `Profile > Settings and activity > Account privacy`, TikTok: `Profile > Settings and privacy > Privacy > Private account`). The number of clicks may also play a role in difficulty of finding a setting. On Instagram and TikTok, users only take 3 and 4 clicks respectively to *audience*, while users on X take 5 clicks.

Second, the UI-path for LinkedIn to *audience* is `Create a post > Who can see your post?`. This path is difficult for users to find, because it is not under the "Settings" section, where users expect to find all settings. Another example is the UI-path for Instagram to *activity status* where it is located inside the "Messages and story replies" section. Almost 65% of Instagram users find the setting hard to locate, which is higher than on other platforms. This highlights that users experience difficulty locating a setting when it is placed under a section with a vague or misleading name.

Recommendations. We recommend a better, more intuitive organization of the privacy settings to improve their discoverability. Specifically, platforms should use precise wording to describe the setting users are trying to adjust. For example, instead of using the click name: "Protect your posts" to represent the setting between public and private account on X, more precise click names such as "Account privacy" on Instagram or "Private account" on TikTok would cause less confusion to users when trying to locate the setting (Table 1). Platforms should also avoid placing privacy settings in the misleading section, for example, placing *activity status* under the section "Messages and story replies" on Instagram. We would like to highlight TikTok's good practice of organizing privacy setting

locations in Table 1. TikTok uses precise and concise wording in all their UI-paths, ensuring settings are placed under the most descriptive sections, which improves discoverability of privacy settings for their users (Section 4.6).

5.2.3 Privacy Regulations.

There is a tussle between what users want (more privacy) and what platforms want (more exposure), as is evident in our results showing that users generally prefer more private settings than platforms' defaults. Platforms seemingly address this by offering various privacy settings for users to adjust. But these settings are not usable, as they are unfamiliar to users and generally difficult to locate. Because interests of users and platforms differ, we cannot just wait for platforms to hear and respond to users' voices. Instead, this is the place where policy and regulations should step in to protect user interests.

Recommendations. We recommend that privacy regulators develop a universal framework to evaluate the usability of platforms' privacy settings. Many studies, including ours, have laid the groundwork for such evaluations. However, these evaluations have mostly been conducted independently. We strongly believe that there is an opportunity to unify these efforts, particularly through collaboration among researchers, regulators, and platforms to establish a universal evaluation framework.

First, we need to define metrics that represent the usability of privacy settings. Ours and work of previous researchers have suggested two potential metrics: (1) Familiarity (awareness) or how well users are aware of and understand the functionality of a given setting, and (2) Accessibility (discoverability) or how easily users can access the setting. Second, we need to develop a scoring system to rank how well each privacy setting performs on these metrics. For example, based on Table 4, we could map a percentage score to a scoring scale between 0 to 10. As a result, the *video* setting on Instagram received a score of 2 for Familiarity and 3 for Accessibility, since only 20% have seen the setting and 34% found it easy to locate. Regulators could develop a policy requiring that each score for every metric must be at least 5. With this requirement, the final step involves regulators routinely running randomized user studies to evaluate the usability of platforms' privacy settings. Since platforms continuously introduce new features or update privacy settings, it is important to ensure these changes consistently comply with the regulations to maintain standard usability for users.

In addition to regulations focused on usability, we recommend that regulators also consider requiring that the default privacy settings be better-aligned with user preferences. When the majority of users prefer the default settings to be more private, the regulators could enforce policies requiring platforms to revise the related defaults. For example, if the regulators define "majority" as 70% of users, then Facebook would be required to adjust the default settings for *ads*, *connection view*, *profile view* and *search engine* to be more private. The regulators would routinely evaluate user preferences to track changes in user populations and trends in how users reason about privacy. Aligning default settings with user preferences would ease the burden on users, and ensure their privacy is protected by default. More importantly, such practice would specifically help users who struggle to find privacy settings as shown in Section 4.4, these users are in fact the ones who care more about their privacy, but face more difficulties in achieving it.

5.2.4 Future Research. While our research sheds light on how unfamiliar users are with privacy settings, and how they struggle to locate them, more research is needed to understand the underlying causes. Specifically, more research is needed to understand how a user's motivation for using a platform (e.g., entertainment, professional networking, etc.) influences their ability to locate some privacy settings. Since our findings show that users' privacy preferences are correlated to their ability to locate settings (Section 4.4), it is important to further explore whether these preferences are shaped by their underlying motivations, potentially revealing a root cause of users' struggles in managing privacy. Additionally, since users that are more active on a platform have more open privacy preferences (Section 4.5), future research is needed to understand if familiarity begets more trust and thus more sharing. Lastly, more longitudinal research is needed to demonstrate that privacy settings are consistently difficult to use. Such evidence could strengthen the case for regulatory intervention, as discussed in Section 5.2.3.

6 Conclusion

We conducted a study (n=541) to measure the user awareness, preferences and usability of social media privacy settings, across six different platforms. We found an industry-wide misalignment between default privacy settings and user preferences. Many users are also unfamiliar with common privacy settings and many, especially older users, struggle to locate them. The more users are unfamiliar with privacy settings, the more they desire privacy and the more they struggle to locate the correct settings. We recommend that platforms adjust their default settings (perhaps driven by regulatory requirements) and that they work on standardizing privacy setting names and locations to improve findability.

Acknowledgments

Research was supported by the Army Research Office (ARO) and accomplished under Cooperative Agreement Number W911NF-20-2-0053. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Army Research Office.

References

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (Aug. 2017), 41 pages. https://doi.org/10.1145/3054926

[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and Human Behavior in the Age of Information. *Science* 347, 6221 (2015), 509–514. https://doi.org/10.1126/science.aaa1465

[3] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2020. Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology* 30, 4 (2020), 736–758. https://doi.org/10.1002/jcpy.1191

[4] Alessandro Acquisti and Ralph Gross. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *Privacy Enhancing Technologies*, George Danezis and Philippe Golle (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 36–58.

[5] A. Acquisti and J. Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy* 3, 1 (2005), 26–33. https://doi.org/10.1109/MSP.2005.22

[6] Alper Alan, Zakwan Al-Arnaout, Ahmet Topcu, Chamseddine Zaki, Ahmed Shdefat, and Ersin Elbasi. 2022. How Do Default Privacy Settings on Social Media Apps Match People's Actual Preferences?. In *2022 International Conference*

on Electrical and Computing Technologies and Applications (ICECTA). 305–308. https://doi.org/10.1109/ICECTA57148.2022.9990282

[7] Mashael Aljohani, Alastair Nisbet, and Kelly Blincoe. 2016. A Survey of Social Media Users Privacy Settings & Information Disclosure. https://doi.org/10.4225/75/58A693DEEE893

[8] Richard A Armstrong. 2014. When to use the Bonferroni correction. https://pubmed.ncbi.nlm.nih.gov/24697967/

[9] Miriam Bartsch and Tobias Dienlin. 2016. Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior* 56 (2016), 147–154. https://doi.org/10.1016/j.chb.2015.11.022

[10] Jeff Bercovici. 2012. Study Shows Women Are Smarter Than Men About Social Media. https://www.forbes.com/sites/jeffbercovici/2012/02/24/study-shows-women-are-smarter-than-men-about-social-media/

[11] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies* 2016 (2016), 237 – 254. https://api.semanticscholar.org/CorpusID:11299521

[12] danah boyd and Eszter Hargittai. 2010. Facebook privacy settings: Who cares? *First Monday* 15, 8 (Jul. 2010). https://doi.org/10.5210/fm.v15i8.3086

[13] Francesco Buccafurri, Lidia Fotia, Gianluca Lax, and Vishal Saraswat. 2016. Analysis-preserving protection of user privacy against information leakage of social-network Likes. *Information Sciences* 328 (2016), 340–358. https://doi.org/10.1016/j.ins.2015.08.046

[14] José González Cabañas, Ángel Cuevas, and Rubén Cuevas. 2018. Unveiling and Quantifying Facebook Exploitation of Sensitive Personal Data for Advertising Purposes. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 479–495. https://www.usenix.org/conference/usenixsecurity18/presentation/cabanas

[15] Pew Research Center. 2012. Privacy management on social media sites: Main findings. https://www.pewresearch.org/internet/2012/02/24/main-findings-12/

[16] Pew Research Center. 2013. Anonymity, Privacy, and Security Online. https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/

[17] Pew Research Center. 2016. The state of privacy in post-Snowden America. https://www.pewresearch.org/short-reads/2016/09/21/the-state-of-privacy-in-america/

[18] Pew Research Center. 2019. Facebook Algorithms and Personal Data. https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/

[19] Pew Research Center. 2021. Social Media Use in 2021. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

[20] Yi Chen, Mingming Zha, Nan Zhang, Dandan Xu, Qianqian Zhao, Xuan Feng, Kan Yuan, Fnu Suya, Yuan Tian, Kai Chen, XiaoFeng Wang, and Wei Zou. 2019. Demystifying Hidden Privacy Settings in Mobile Apps. In *2019 IEEE Symposium on Security and Privacy (SP)*. 570–586.

[21] Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung. 2018. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior* 81 (2018), 42–51.

[22] Taejoong Chung, Jinyoung Han, Daejin Choi, Ted Taekyoung Kwon, Jong-Youn Rha, and Hyunchul Kim. 2017. Privacy Leakage in Event-based Social Networks: A Meetup Case Study. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 35 (Dec. 2017), 22 pages. https://doi.org/10.1145/3134670

[23] Jessica Colnago, Lorrie Faith Cranor, and Alessandro Acquisti. 2023. Is There a Reverse Privacy Paradox? An Exploratory Analysis of Gaps Between Privacy Perspectives and Privacy-Seeking Behaviors. *Proceedings on Privacy Enhancing Technologies Symposium* 2023, 1 (July 2023), 455–476. Available at SSRN: https://ssrn.com/abstract=4607259.

[24] Jessica Colnago, Lorrie Faith Cranor, Alessandro Acquisti, and Kate Hazel Stanton. 2022. Is it a concern or a preference? An investigation into the ability of privacy scales to capture and distinguish granular privacy constructs. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 331–346. https://www.usenix.org/conference/soups2022/presentation/colnago

[25] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 407, 24 pages. https://doi.org/10.1145/3491102.3517504

[26] Emily Geisen. 2022. Improve data quality by using a commitment request instead of attention checks. *Qualtrics* (August 2022). https://www.qualtrics.com/blog/attention-checks-and-data-quality.

[27] Guardian21. 2021. Joe Biden's Venmo account discovered in 'less than 10 minutes' – report. https://www.theguardian.com/us-news/2021/may/15/biden-venmo-account-buzzfeed-news-national-security

[28] Tobias Gummer, Joss Roßmann, and Henning Silber. 2021. Using Instructed Response Items as Attention Checks in Web Surveys: Properties and Implementation. *Sociological Methods & Research* 50 (06 2021), 004912411876908. https://doi.org/10.1177/0049124118769083

[29] Isobel Asher Hamilton. 2019. TikTok was bigger than Instagram last year after passing the 1 billion download mark. https://www.businessinsider.com/tiktok-hit-1-billion-downloads-surpassing-instagram-in-2018-2019-2

[30] Silas Hsu, Kristen Vaccaro, Yin Yue, Aimee Rickman, and Karrie Karahalios. 2020. Awareness, Navigation, and Use of Feed Control Settings Online. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376583

[31] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. 2015. Face/Off: Preventing Privacy Leakage From Photos in Social Networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (Denver, Colorado, USA) *(CCS '15)*. Association for Computing Machinery, New York, NY, USA, 781–792. https://doi.org/10.1145/2810103.2813603

[32] Instagram. 2020. Introducing Instagram Reels. https://about.instagram.com/blog/announcements/introducing-instagram-reels-announcement

[33] The Wall Street Journal. 2023. We Aren't Posting on Social Media as Much Anymore. Will We Ever? https://www.wsj.com/tech/personal-tech/social-media-nobody-posting-f6c2fd3e

[34] Munene Kanampiu and Mohd Anwar. 2019. Privacy Preferences vs. Privacy Settings: An Exploratory Facebook Study. In *Advances in Human Factors in Cybersecurity*, Tareq Z. Ahram and Denise Nicholson (Eds.). Springer International Publishing, Cham, 116–126.

[35] Dilara Keküllüoglu, Walid Magdy, and Kami Vaniea. 2020. Analysing Privacy Leakage of Life Events on Twitter. In *Proceedings of the 12th ACM Conference on Web Science* (Southampton, United Kingdom) *(WebSci '20)*. Association for Computing Machinery, New York, NY, USA, 287–294. https://doi.org/10.1145/3394231.3397919

[36] Dilara Kekulluoglu, Kami Vaniea, and Walid Magdy. 2022. Understanding Privacy Switching Behaviour on Twitter. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 31, 14 pages. https://doi.org/10.1145/3491102.3517675

[37] Dilara Keküllüoğlu, Walid Magdy, and Kami Vaniea. 2022. From an Authentication Question to a Public Social Event: Characterizing Birthday Sharing on Twitter. *Proceedings of the International AAAI Conference on Web and Social Media* 16, 1 (May 2022), 488–499. https://doi.org/10.1609/icwsm.v16i1.19309

[38] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 3393–3402. https://doi.org/10.1145/2470654.2466466

[39] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64 (2017), 122–134. https://doi.org/10.1016/j.cose.2015.07.002

[40] Balachander Krishnamurthy, Konstantin Naryshkin, and Craig Wills. 2011. Privacy leakage vs. protection measures: the growing disconnect. In *Proceedings of the Web*, Vol. 2. 1–10.

[41] Balachander Krishnamurthy and Craig E Wills. 2008. Characterizing privacy in online social networks. In *Proceedings of the first workshop on Online social networks*. 37–42.

[42] Balachander Krishnamurthy and Craig E. Wills. 2009. On the leakage of personally identifiable information via online social networks. In *Proceedings of the 2nd ACM Workshop on Online Social Networks* (Barcelona, Spain) *(WOSN '09)*. Association for Computing Machinery, New York, NY, USA, 7–12. https://doi.org/10.1145/1592665.1592668

[43] Huaxin Li, Haojin Zhu, Suguo Du, Xiaohui Liang, and Xuemin Shen. 2016. Privacy leakage of location sharing in mobile social networks: Attacks and defense. *IEEE Transactions on Dependable and Secure Computing* 15, 4 (2016), 646–660.

[44] Yabing Liu, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove. 2011. Analyzing facebook privacy settings: user expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (Berlin, Germany) *(IMC '11)*. Association for Computing Machinery, New York, NY, USA, 61–70. https://doi.org/10.1145/2068816.2068823

[45] Byron Lowens, Sean Scarnecchia, Jane Im, Tanisha Afnan, Annie Chen, Yixin Zou, and Florian Schaub. 2025. Misalignments and Demographic Differences in Expected and Actual Privacy Settings on Facebook. *Proceedings on Privacy Enhancing Technologies* 2025, 1 (2025), 456–471.

[46] Michelle Madejski, Maritza Johnson, and Steven Bellovin. 2011. The Failure of Online Social Network Privacy Settings.

[47] Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. 2012. A study of privacy settings errors in an online social network. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. 340–345. https://doi.org/10.1109/PerComW.2012.6197507

[48] Mainack Mondal, Günce Su Yilmaz, Noah Hirsch, Mohammad Taha Khan, Michael Tang, Christopher Tran, Chris Kanich, Blase Ur, and Elena Zheleva. 2019. Moving Beyond Set-It-And-Forget-It Privacy Settings on Social Media. In *Proceedings*

of the 2019 ACM SIGSAC Conference on Computer and Communications Security (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 991–1008. https://doi.org/10.1145/3319535.3354202

[49] Rachel E. Morgan and Jennifer L. Truman. 2022. Stalking Victimization, 2019. https://bjs.ojp.gov/content/pub/pdf/sv19.pdf

[50] Guillaume Nadon, Marcus Feilberg, Mathias Johansen, and Irina Shklovski. 2018. In the User We Trust: Unrealistic Expectations of Facebook's Privacy Mechanisms. In *Proceedings of the 9th International Conference on Social Media and Society* (Copenhagen, Denmark) *(SMSociety '18)*. Association for Computing Machinery, New York, NY, USA, 138–149. https://doi.org/10.1145/3217804.3217906

[51] Michel Netter, Moritz Riesner, Michael Weber, and Günther Pernul. 2013. Privacy Settings in Online Social Networks – Preferences, Perception, and Reality. In *2013 46th Hawaii International Conference on System Sciences*. 3219–3228. https://doi.org/10.1109/HICSS.2013.455

[52] X Daily News. 2023. NEWS: X/Twitter will now let you choose if others can download your videos! https://x.com/xDaily/status/1686780907686969362

[53] Stefanie Pötzsch. 2009. Privacy Awareness: A Means to Solve the Privacy Paradox?. In *The Future of Identity in the Information Society*, Vashek Matyáš, Simone Fischer-Hübner, Daniel Cvrček, and Petr Švenda (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 226–236.

[54] Qualtrics. 2025. Timing Question. https://www.qualtrics.com/support/survey-platform/survey-module/editing-questions/question-types-guide/advanced/timing/

[55] Emilee Rader. 2014. Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 51–67. https://www.usenix.org/conference/soups2014/proceedings/presentation/rader

[56] Emilee Rader, Samantha Hautea, and Anjali Munasinghe. 2020. "I Have a Narrow Thought Process": Constraints on Explanations Connecting Inferences and Self-Perceptions. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 457–488. https://www.usenix.org/conference/soups2020/presentation/rader

[57] Kopo M. Ramokapane, Anthony C. Mazeli, and Awais Rashid. 2019. Skip, Skip, Skip, Accept!!!: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy. *Proceedings on Privacy Enhancing Technologies* 2019, 2 (April 2019), 209–227. https://doi.org/10.2478/popets-2019-0027

[58] Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. 2016. Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 77–96. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/rao

[59] Reuters. 2025. Facebook defends $725 million privacy settlement in US appeals court. https://www.reuters.com/legal/litigation/facebook-defends-725-million-privacy-settlement-us-appeals-court-2025-02-07/

[60] Agrima Srivastava and G Geethakumari. 2013. Measuring privacy leaks in Online Social Networks. In *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. 2095–2100. https://doi.org/10.1109/ICACCI.2013.6637504

[61] Statista. 2024. Most popular social networks worldwide as of April 2024, by number of monthly active users. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[62] Statista. 2025. Number of internet and social media users worldwide as of February 2025. https://www.statista.com/statistics/617136/digital-population-worldwide/

[63] Rajat Tandon, Pithayuth Charnsethikul, Ishank Arora, Dhiraj Murthy, and Jelena Mirkovic. 2022. I know what you did on Venmo: Discovering privacy leaks in mobile social payments. *Proceedings on Privacy Enhancing Technologies* 2022 (2022), 200–221. https://api.semanticscholar.org/CorpusID:249878422

[64] Threatpost. 2021. Data for 700M LinkedIn Users Posted for Sale in Cyber-Underground. https://threatpost.com/data-700m-linkedin-users-cyber-underground/167362/

[65] Virpi Kristiina Tuunainen, Olli Pitkänen, and Marjaana Hovi. 2009. Users' Awareness of Privacy on Online Social Networking Sites - Case Facebook. In *BLED eConference*. BLED. https://api.semanticscholar.org/CorpusID:31844121

[66] Maria Han Veiga and Carsten Eickhoff. 2016. Privacy Leakage through Innocent Content Sharing in Online Social Networks. arXiv:1607.02714 [cs.SI] https://arxiv.org/abs/1607.02714

[67] Na Wang, Pamela Wisniewski, Heng Xu, and Jens Grossklags. 2014. Designing the default privacy settings for facebook applications. In *Proceedings of the Companion Publication of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Baltimore, Maryland, USA) *(CSCW Companion '14)*. Association for Computing Machinery, New York, NY, USA, 249–252. https://doi.org/10.1145/2556420.2556495

[68] Jason Watson, Heather Richter Lipford, and Andrew Besmer. 2015. Mapping User Preference to Privacy Default Settings. *ACM Trans. Comput.-Hum. Interact.* 22, 6, Article 32 (Nov. 2015), 20 pages. https://doi.org/10.1145/2811257

[69] Lauren E Willis. 2014. Why not privacy by default? *Berkeley Tech. LJ* 29 (2014), 61.

[70] Heng Xu, Xin (Robert) Luo, John M. Carroll, and Mary Beth Rosson. 2011. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems* 51, 1 (2011), 42–52. https://doi.org/10.1016/j.dss.2010.11.017

[71] Lingjing Yu, Sri Mounica Motipalli, Dongwon Lee, Peng Liu, Heng Xu, Qingyun Liu, Jianlong Tan, and Bo Luo. 2018. My Friend Leaks My Privacy: Modeling and Analyzing Privacy in Social Networks. In *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies* (Indianapolis, Indiana, USA) *(SACMAT '18)*. Association for Computing Machinery, New York, NY, USA, 93–104. https://doi.org/10.1145/3205977.3205981

A Informed Consent

We are conducting a research study to understand user preferences towards social media privacy settings. We are seeking your participation in this study. Your participation is completely voluntary, and we will address your questions or concerns at any point before or during the study.

You may be eligible to participate in this study if you meet the following criteria:

(1) You are over 18 years old.
(2) You are currently having a social media account(s) and using it regularly.

If you decide to participate in this study, you will be asked to do the following activities:

(1) Select any social media platform(s) from the list (Facebook, Instagram, Twitter (X), LinkedIn, TikTok, LinkedIn, and Snapchat) that you are currently having an account on and use regularly.
(2) Answer a series of questions about your privacy preferences and locating privacy settings on the platform.
(3) Provide demographic information via multiple choices where each choice represents a range including age, gender, education, and region.

You'll need a phone with your account open for references when locating privacy settings. You don't need to have extensive knowledge in social media or privacy settings to complete this study.

The survey takes approximately 15-20 minutes. After you complete it, you will receive a compensation of $3.00. We will manually review your effort before sending out the compensation via Prolific.

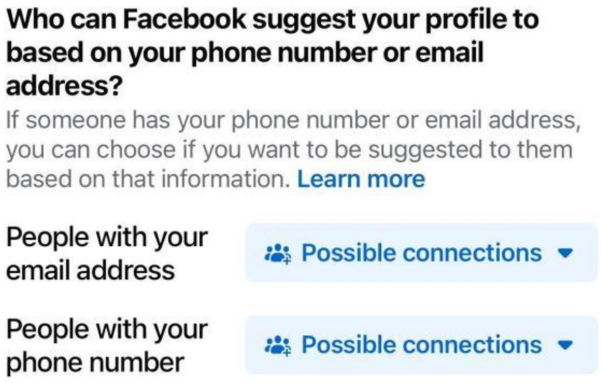
Our research group will publish the results in conference and journal publications. Participants will not be identified in the results. We will take reasonable measures to protect the security of all your personal information. All data will be de-identified prior to any publication or presentations. We may share de-identified data with other researchers in the future.

B Survey

All survey questionnaires can be found at https://drive.google.com/file/d/1yfntYpiQOdhizxyu_b7BzrTzWC2SZO6b/view?usp=sharing. We provide survey question examples below:

B.1 Awareness Question

Have you ever seen this privacy feature: **Profile Suggestion (i.e., suggesting your profile to other Facebook users who have your email or phone number)**?



- ☐ Yes, I've seen it
- ☐ No, I've never seen it

B.2 Preference Question

By default, your profile WILL be suggested to people who have your email or phone number.
Are you satisfied with this default setting?

- ☐ Yes, I am satisfied with the default setting
- ☐ No, I prefer it to be more PRIVATE (e.g., your profile won't be suggested to people who have your email or phone number)

B.3 Discoverability Section

Please locate the privacy feature that prevents people from seeing when you are active on Facebook (**Activity Status**).

Note each click you make starting from your feed to locate **Activity Status**, whether or not it takes you to the destination.

Can you locate **Activity Status**?

- ☐ Yes
- ☐ No

Rate how hard to locate **Activity Status**.

- ☐ Very Difficult
- ☐ Difficult
- ☐ Moderate
- ☐ Easy
- ☐ Very Easy

B.4 Commitment Request Question

We care about the quality of our survey data. Therefore, it is important that you provide accurate answers to every question in this survey.

Have you provided accurate answers to the previous questions in this survey, and will you continue to do so for the remaining questions?

- ☐ I am not sure
- ☐ Yes, I have and I will
- ☐ No, I will not

B.5 Additional Results

We ran linear regression models to test for differences across *platforms*, and how they might depend on the *age* factor. Each regression is treated as a separate test for each dependent variable. Therefore, we do not apply correction in this analysis and use 0.05 as the significance threshold. We use the notation, β_{int}, to describe the interaction significance.

P_SEEN: platform significantly interacts with *age* to predict the percentage of privacy settings a user has seen, given X as a reference platform ($0.181 \leq |\beta| \leq 0.340$, $p \leq 0.030$). Simple effects tests show that, among the older participants, X users have, on average, seen 13-36% fewer privacy settings compared to users of other platforms ($0.132 \leq |\beta| \leq 0.360$, $p \leq 0.028$).

P_PRIVATE: platform significantly interacts with *age* to predict the percentage of privacy settings a user prefers to be more private than the default, given LinkedIn as a reference platform ($|\beta| = 0.137$, $p = 0.047$) Simple effects tests show that, among the younger participants, TikTok users prefer, on average, 21% more of their privacy settings to be more private than the default compared to LinkedIn users ($|\beta| = 0.206$, $p < 0.0001$).

P_HARD: platform significantly interacts with *age* to predict the percentage of privacy settings a user feels are hard to locate, given X as a reference platform ($0.128 \leq |\beta| \leq 0.168$, $p \leq 0.030$). Simple effects tests show that, among the younger participants, X users find, on average, 10-23% more of their privacy settings hard to locate compared to users of other platforms ($0.100 \leq |\beta| \leq 0.227$, $p \leq 0.037$). Similarly, among the older participants, X users find, on average, 27-35% more of their privacy settings hard to locate compared to users of other platforms ($0.269 \leq |\beta| \leq 0.354$, $p \leq 0.0001$).

A_TIME: platform significantly interacts with *age* to predict the average number of seconds a user spends locating a privacy setting, given LinkedIn as a reference platform ($38.873 \leq |\beta| \leq 52.310$, $p \leq 0.036$). Simple effects tests show that, among the younger participants, LinkedIn users spend 24-58 seconds more to locate privacy settings compared to users of other platforms ($24.116 \leq |\beta| \leq 57.996$, $p \leq 0.024$). However, among the older participants, Facebook users spend 28 seconds more to locate privacy settings compared to LinkedIn users ($|\beta| = 27.659$, $p = 0.010$).

C Additional Figures and Tables

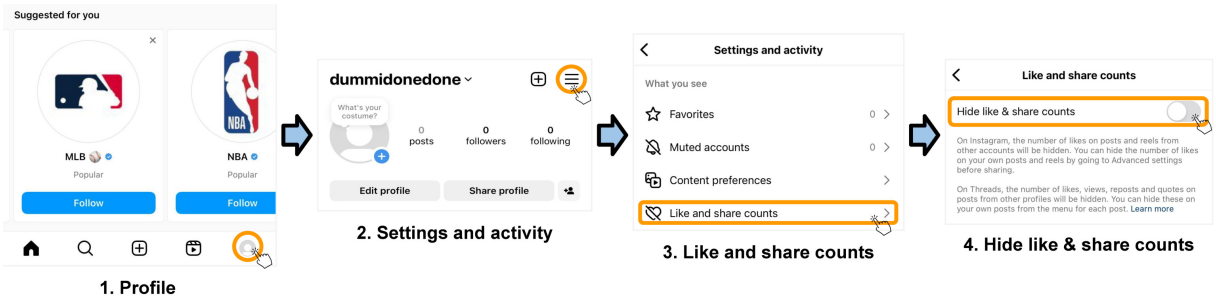


Figure 4: A UI-path or a series of clicks starting from the user's feed to the given privacy setting, e.g., hiding like and share counts on Instagram.

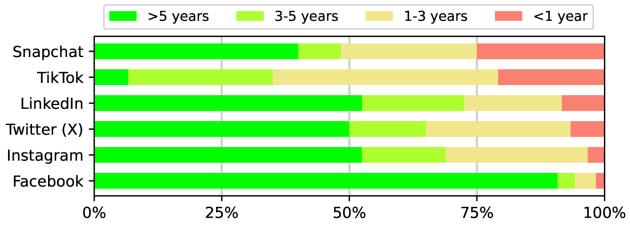


Figure 5: The number of years a participant has been using the platform.

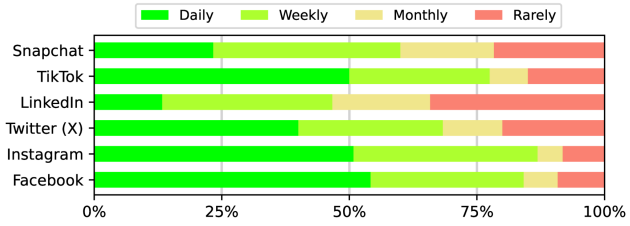


Figure 6: Usage frequency on the platform.

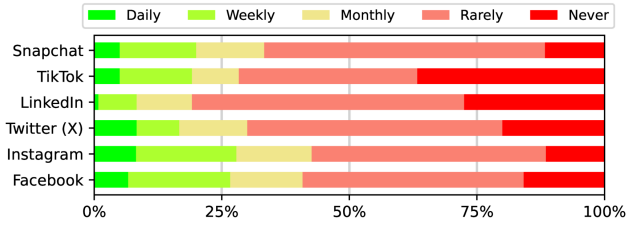


Figure 7: Post and sharing frequency on the platform.

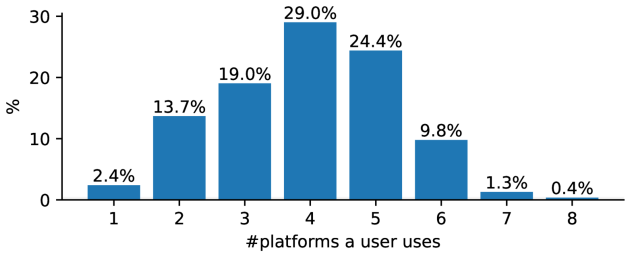


Figure 8: The number of platforms a participant uses.

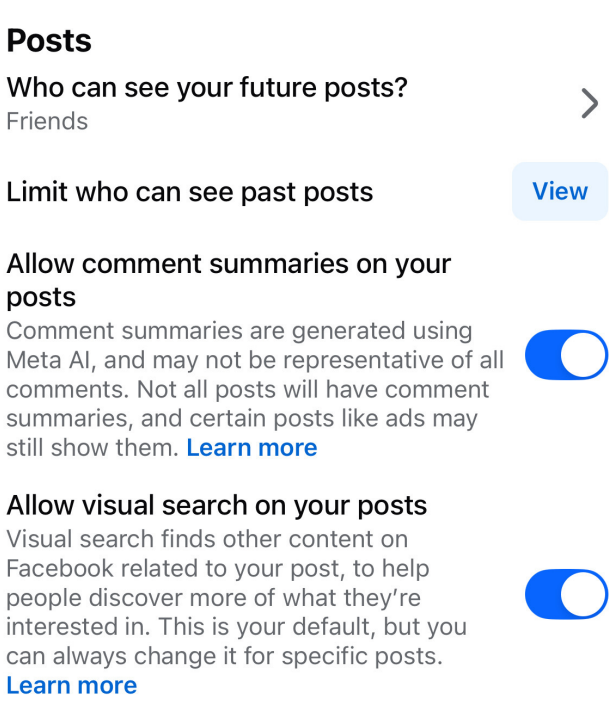


Figure 9: Facebook's post setting.

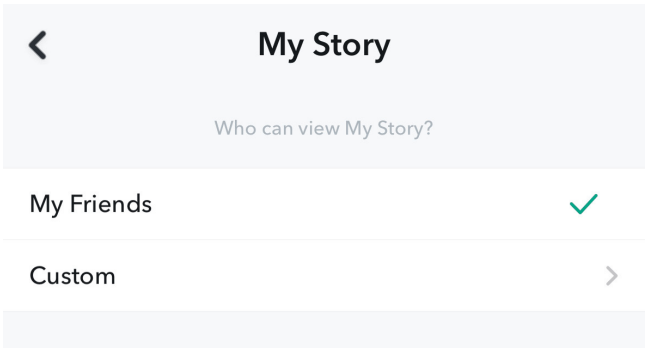


Figure 10: Snapchat's story setting.

Table 5: The number of mobile OS participants used for locating privacy settings in the study.

	Num. (%)		
Platform	Android	iOS	Others
Facebook	80 (67%)	39 (32%)	1 (1%)
Instagram	34 (56%)	27 (44%)	0 (0%)
X	40 (67%)	19 (32%)	1 (1%)
LinkedIn	76 (63%)	43 (36%)	1 (1%)
TikTok	74 (62%)	46 (38%)	0 (0%)
Snapchat	33 (55%)	27 (45%)	0 (0%)
Total	337 (62%)	201 (37%)	3 (1%)

Table 6: Linear regression between demographic and usage independent variables (with reference groups in parentheses) and dependent variables (DV), including the percentage of privacy settings a user has seen (*P_SEEN*), prefers to be more private (*P_PRIVATE*), feels are hard to locate (*P_HARD*), and the average number of seconds a user spends locating a privacy setting (*A_TIME*). The following parameters are produced by Ordinary Least Squares: β or coefficient, SE or Standard Error, t or t-value, CI or Confidence Interval. We only show the variables with significant differences.

Comparison	DV	β	SE	t	95% CI	p-value
age: 45+ (vs. 18 – 44)	*P_SEEN*	-0.101	0.024	-4.232	[-0.147, -0.054]	**<0.0001*****
	P_HARD	0.052	0.018	2.840	[0.016, 0.088]	0.005**
	A_TIME	10.500	5.240	2.000	[0.206, 20.794]	0.046*
gender: Male (vs. Female)	*P_PRIVATE*	-0.079	0.024	-3.291	[-0.126, -0.032]	**0.001*****
tech background: Yes (vs. No)	*P_PRIVATE*	-0.068	0.026	-2.631	[-0.118, -0.017]	0.009**
usage freq: <Weekly (vs. Daily)	*P_HARD*	0.069	0.022	3.091	[0.025, 0.113]	**0.002*****
post freq: >=Monthly (vs. <Monthly)	*P_SEEN*	0.056	0.026	2.163	[0.005, 0.107]	0.031*
	P_PRIVATE	-0.090	0.026	-3.487	[-0.14, -0.039]	**<0.001*****
os: iOS (vs. Android)	*A_TIME*	-15.830	5.413	-2.925	[-26.462, -5.197]	0.004**
#platforms	*P_SEEN*	0.029	0.009	3.196	[0.011, 0.047]	**0.001*****
	P_PRIVATE	-0.033	0.009	-3.676	[-0.051, -0.015]	**<0.001*****

Significant thresholds: **p*** < 0.0036 (correction)**, p** < 0.01, p* < 0.05 (default)

Table 7: Linear regression between the independent variable "platform" (with reference groups in parentheses) and the same dependent variables (DVs) as shown in Table 6. Please refer to other abbreviations in Table 6. We only show the variables with significant differences.

Comparison	DV	β	SE	t	95% CI	p-value
(Facebook vs.) Instagram	*P_SEEN*	-0.112	0.043	-2.595	[-0.197, -0.027]	0.010*
(Facebook vs.) X		-0.142	0.043	-3.277	[-0.227, -0.057]	**0.001****
(Facebook vs.) LinkedIn		-0.101	0.035	-2.854	[-0.171, -0.031]	0.004**
(Instagram vs.) TikTok		0.124	0.043	2.878	[0.039, 0.209]	0.004**
(Instagram vs.) Snapchat		0.160	0.050	3.205	[0.062, 0.258]	**0.001****
(X vs.) TikTok		0.154	0.043	3.558	[0.069, 0.239]	**<0.001****
(X vs.) Snapchat		0.190	0.050	3.795	[0.092, 0.288]	**<0.001****
(LinkedIn vs.) TikTok		0.113	0.035	3.199	[0.044, 0.183]	**0.001****
(LinkedIn vs.) Snapchat		0.149	0.043	3.435	[0.064, 0.234]	**<0.001****
(Facebook vs.) X	*P_PRIVATE*	-0.158	0.042	-3.732	[-0.242, -0.075]	**<0.001****
(Facebook vs.) LinkedIn		-0.235	0.035	-6.796	[-0.303, -0.167]	**<0.0001****
(Facebook vs.) TikTok		-0.098	0.035	-2.818	[-0.166, -0.030]	0.005**
(Facebook vs.) Snapchat		-0.095	0.042	-2.239	[-0.178, -0.012]	0.026*
(Instagram vs.) X		-0.140	0.049	-2.867	[-0.236, -0.044]	0.004**
(LinkedIn vs.) Instagram		0.217	0.042	5.142	[0.134, 0.300]	**<0.0001****
(LinkedIn vs.) TikTok		0.138	0.035	3.978	[0.070, 0.206]	**<0.0001****
(LinkedIn vs.) Snapchat		0.140	0.042	3.310	[0.057, 0.224]	**0.001****
(Facebook vs.) Snapchat	*P_HARD*	0.071	0.030	2.397	[0.013, 0.129]	0.017*
(Instagram vs.) Facebook		-0.227	0.029	-7.700	[-0.285, -0.169]	**<0.0001****
(Instagram vs.) LinkedIn		-0.211	0.029	-7.170	[-0.269, -0.153]	**<0.0001****
(Instagram vs.) Snapchat		-0.156	0.034	-4.575	[-0.223, -0.089]	**<0.0001****
(X vs.) Facebook		-0.201	0.030	-6.783	[-0.259, -0.143]	**<0.0001****
(X vs.) LinkedIn		-0.185	0.030	-6.255	[-0.244, -0.127]	**<0.0001****
(X vs.) Snapchat		-0.130	0.034	-3.798	[-0.197, -0.063]	**<0.001****
(TikTok vs.) Facebook		0.089	0.024	3.695	[0.042, 0.137]	**<0.001****
(TikTok vs.) Instagram		0.316	0.029	10.734	[0.259, 0.374]	**<0.0001****
(TikTok vs.) X		0.290	0.030	9.800	[0.232, 0.349]	**<0.0001 ****
(TikTok vs.) LinkedIn		0.105	0.024	4.341	[0.058, 0.153]	**<0.0001****
(TikTok vs.) Snapchat		0.161	0.030	5.414	[0.102, 0.219]	**<0.0001****
(Facebook vs.) Instagram	*A_TIME*	-19.356	9.340	-2.072	[-37.704, -1.009]	0.039*
(Facebook vs.) X		-19.665	9.391	-2.094	[-38.113, -1.216]	0.037*
(Facebook vs.) TikTok		-34.606	7.668	-4.513	[-49.669, -19.543]	**<0.0001**
(Facebook vs.) Snapchat		-38.701	9.391	-4.121	[-57.150, -20.253]	**<0.0001**
(LinkedIn vs.) TikTok		-33.036	7.668	-4.308	[-48.099, -17.973]	**<0.0001**
(LinkedIn vs.) Snapchat		-37.131	9.391	-3.954	[-55.579, -18.683]	**<0.0001**

Significant thresholds: **p*** < 0.0036 (correction)**, p** < 0.01, p* < 0.05 (default)