Evaluating and Comparing the Usability of Privacy in WhatsApp, Twitter, and Snapchat

Abdulmohsen S. Albesher[1]
Information Systems Department
King Faisal University, Alahsa
Saudi Arabia

Thamer Alhussain[2]
E-Commerce Department
Saudi Electronic University
Riyadh, Saudi Arabia

***Abstract*—With the increased use of social networking platforms, especially with the inclusion of sensitive personal information, it has become important for those platforms to have adequate levels of security and privacy. This research aimed to evaluate the usability of privacy in the WhatsApp, Twitter, and Snapchat applications. The evaluation was conducted based on the structured analysis of privacy (STRAP) framework. Seven expert evaluators performed heuristic evaluations and applied the 11 STRAP heuristics to the privacy policy statements and settings provided in the WhatsApp, Twitter, and Snapchat applications. This study provides useful information for designers and developers of social media applications as well as users of the apps. In particular, the results indicate that Snapchat had the highest severity rating, followed by Twitter and WhatsApp. Moreover, the most notable severity rating for all the apps was regarding the ability to revoke consent, where all of the apps had a very high number of usability problems.**

Keywords*—*HCI; usability; heuristics evaluation; STRAP; privacy; usable privacy; social media

I. Introduction

Individuals are becoming more reliant on social media platforms as essential mediums for communication. The global average penetration rate for social media increased from 40% in 2018 to 49% in 2020 [1]. In other words, more than three billion people use social media. Most social media users prefer to connect to their accounts using an application (app) on their smartphones [1], [2]. Social media platforms provide individuals with ways to interface and offer information and snapshots of their lives.

As the commitment of users to social networking platforms expands, the volume of private and personal data that is shared online increases in a like manner. While these platforms offer privacy settings so that users can secure their online privacy, several reports (as cited in [3]) have shown that the average social media user does not change his or her security settings. A lack of public knowledge has resulted in the intermittent use of these settings by many users. Albesher and Alhussain [4] discussed the reasons for not adjusting privacy settings, which included a lack of awareness of the possible risks, the time it takes to read and understand each setting, and the diversity of the settings.

This paper contributes to the knowledge of understanding the term “usable privacy” and how it can improve the usability of privacy settings and policies in social media. As a result, users would deal with these settings and policies effectively and efficiently. Comparing the privacy settings and policies of three different examples of the most popular social media grants practical ideas for improving the design of usable privacy settings and policies. This comparison becomes more useful when a trustable framework is applied. This paper evaluates the usability of privacy settings and policies in the WhatsApp, Twitter, and Snapchat apps within the structured analysis of privacy (STRAP) framework [5]. It further contributes to the existing knowledge on online privacy by testing the STRAP framework in the usability of privacy context. The study provides useful information for designers and developers of social media applications as well as users of the apps to enhance the usability of privacy. All the investigated apps could involve similar privacy issues, and it is a user’s responsibility to carefully adjust the privacy settings to protect his or her information. Although WhatsApp looks simple in terms of usage, it could present several privacy issues because it allows communication with unknown people. Users are responsible for deciding who can see their personal information, such as their profile photos and “about” sections. Conversely, while Twitter and Snapchat appear to be public networks, they allow users to keep their private information hidden from the public. A consequence of that policy is that users can control several aspects of privacy when selecting options for their privacy settings in those apps.

The paper is structured as follows. Section II introduces usability and privacy, followed by more details about the usability of privacy in social media. Next, Section III describes and justifies the research methodology used in this study, and the data collection methods used is presented. Section IV presents and discusses the main results, and Section V presents the conclusion.

II. Literature Review

A. Usability

Usability is a well-known concept in design. Recently, usability has become a popular term when designing privacy policies and settings. Generally, the usability of a system refers to the measure of certain metrics, such as the ease of use and efficiency of that system. Similarly, the usability of a private setting or policy means measuring the ease of reading, locating, and adjusting that setting [6]. A potentially appropriate definition of usability for all fields of study could be “an evaluation of the level of quality of a user’s experience (UX)” because UX has a broader meaning [6]. In fact, Don Norman indicated that UX covers different parts of the interaction between users and systems. This interaction includes industrial design graphics, interfaces, physical interactions, and manuals [7].

B. Privacy

Privacy has different definitions and they are varied depending on the entity that is protected. Nonetheless, privacy has general definitions that could be broad enough to cover many privacy issues. One example is the definition by Oxford English Dictionary (as cited in [8]) which defined privacy as the “state or condition of being free from being observed or disturbed by other people”. Another example was brought by Warren & Brandeis [9] which is “the right to be left alone”. On the other hand, there are specific definitions for specific entities such as information privacy. According to Miltgen and Smith [10], information privacy concerns the security of personal or private data and, as a rule, identifies individual information stored on PC frameworks. For the most part, Miltgen and Smith [10] insisted that information privacy is viewed as a significant part of data and information sharing. This position is based on, for example, the view that, given the headway made in the digital age, personal and private data vulnerabilities have expanded. Similarly, Choi, Park, and Jung [11] stated that information privacy is already applicable in many forms that aim to secure personal user data. These researchers further indicated that information privacy might be applied through various means, including encryption, data and information masking, or authentication—each to guarantee that data are accessible to only those with approved access. These defensive measures are designed to forestall information mining and the unapproved utilization of individuals’ data.

More particular, there are some specific definitions for privacy that can be very useful for the case of protecting personal information in social media. For instance, Bünnig and Cap [12] defined privacy as “protecting personal information from being misused by malicious entities and allowing certain authorized entities to access that personal information by making it visible to them” (as cited in [13]). Additionally, Alan Westin [9] described privacy as the right to let people decide when, how, and to what extent their information is exposed to others (as cited in [14]).

C. Privacy Settings

When people register for social media, they are presented with certain privacy policies and settings; in this context, privacy settings refer to the restriction of the disclosure of shared content to only authorized people [3]. Users could be considered the authors of the settings, but then different usability problems could occur [15]. Indeed, more usable privacy settings lead to experiences that better meet users’ preferences and needs [16]. Akcora and Ferrari [17] posited that users will make poor decisions about their private information when they must deal with many options in privacy settings.

Kane [18] observed that social networking platforms offer people simple approaches to interacting online, making new companions, and staying in contact with existing connections. Nonetheless, Kane [18] asserted that in meeting individuals on the internet with whom one has no prior acquaintance, a user encounters certain inherent risks. Kane [18] insisted that users, when talking and sharing ideas and information online, should remember that once a message, photograph, or video is shared, they no longer have any influence over where it goes. Trottier [19] asserted that the need for privacy settings emerged because of that feature. Privacy settings are control mechanisms accessible on social networking platforms and sites that permit clients to limit who can see their profiles and filter what data or information other users or guests can see. Put simply, privacy settings help guarantee that online users have control over the friends they choose to accept online and whether the information they share is made public or not.

D. Usability of Privacy

The usability of privacy is not a new concept although scholars used slightly different terms to refer to this concept. For example, Aldhafferi et al. [13] mentioned the term “privacy by design” and defined it as granting more authority to users to specify what type of information they want to share and with whom. Another term that has a similar meaning is “usable security,” which refers to whether an app grants its users enough information to make informed decisions about who can access their data and with whom it is shared (as cited in [20]).

Over the last decades, use of the term “usable privacy” has increased rapidly because there has been a significant increase in the number of research papers studying this term [21]. In fact, there are well-known conferences such as the Symposium On Usable Privacy and Security (SOUPS) that are conducted to encourage researchers to publish in this area. Additionally, there are specific courses in highly ranked universities such as Carnegie Mellon University and the University of California-Berkeley that are named “usable privacy and security”.

Some scholars have defined usable privacy as the ability of users to locate, understand, and successfully use privacy controls to protect their privacy [22]. Thus, developers should design interfaces that help users protect their privacy through alignment with this concept. By applying the fundamentals of user-centered design to privacy, organizations can enhance their users’ trust and avoid legal issues [22].

There are several research papers and projects related to usable privacy. For instance, Raschke et al. [23] relied on usability engineering lifecycles that were created by Nielsen and Möller to evaluate privacy. They aimed to design a usable privacy dashboard that could manage the requirements of the General Data Protection Regulation (GDPR). Additionally, Sadeh et al. [24] aimed to achieve usable privacy policies by combining crowdsourcing, machine learning, and natural language. In this project, they relied on the principles of iterative, user-centered design. Moreover, Angulo et al. [25] proposed an approach for designing usable interfaces for privacy policies to assist users in making mindful decisions regarding the dispersal of their personal information. This approach relied on predefined levels of privacy settings. Furthermore, Jones et al. [26] designed a prototype for privacy policies for a British media service. This prototype created a new interactive design that helped users make informed decisions about their data usage. The results showed that users were more comfortable with the new design, which had positive effects on their trust in the media service.

E. Usability of Privacy Settings in Social Media

Privacy settings are a central issue for users of social media. Fiesler et al. [27] indicated that the principal choice users must be aware of when they are creating accounts on Twitter is whether they will post secure tweets or open tweets. The secured tweet highlight implies that nobody other than a user's permitted followers will see the user's messages. It also means that other users will not be able to retweet the user's messages or post them to their streams. If a user picks a secured account, the user can also generally change it later to an open account in the privacy settings. However, it should be noted that Twitter fails to offer the same degree of granular control as other social media platforms. Regardless, it has some better-than-average choices for controlling what different clients can see and what level of access they need to interact with another user. These settings are more for controlling tweets that are sensitive, both the tweets a user creates and the tweets a user views. Accordingly, Twitter permits clients to not only block delicate media but also mark something they are going to post as sensitive. For instance, the privacy setting "Safety" is the place where users can choose to reject tweets that are offensive or unwanted, as well as mute or block accounts. Likewise, there are privacy settings that allow users to select, for instance, a setting to "receive anybody" or the option to allow read receipts.

Dev, Das, and Camp [28] indicated that WhatsApp settled on a security decision dependent on usability because it had 1 billion clients and closing down conversations could be irritating for many clients. This means that the entire framework may be less secure. However, although most clients know that they can modify their WhatsApp privacy settings, the majority only use the privacy options "everybody" or "my contacts," conceivably on the grounds that they want to permit family and friends to see whatever they post online. While there are other options in the privacy settings for WhatsApp, most WhatsApp's clients use only the basic settings, indicating that the use of the privacy settings is not that common for users.

Furthermore, WhatsApp offers its users the ability to control who can access their online data. Regardless of whether users decide to limit access to their data, they are given the option to choose a specific setting, for example, to display their online data either to their entire contact list or to no one else under any circumstances. Dev, Das, and Camp [28] appeared to insist that a user can change who has permission to view the user's profile photograph, "about" message, and status in the privacy settings, with differing results for the various choices. For instance, if a user hides the "Last Seen" setting, it means that the user's contacts will not see when the user last logged into WhatsApp. Conversely, even if a user does not use this degree of protection, he or she should be aware that others might.

In contrast, Snapchat is tremendously well known for its privacy settings, as Mondal et al. [29] articulated. Snapchat's prevalence implies that if users are not cautious, they will undoubtedly receive snaps, invites, spam, or even calls from random individuals—unless they secure their privacy on Snapchat. There are a few settings for enabling or disabling Snapchat features that will successfully forestall all the issues mentioned above. Mondal et al. [29] mentioned that Snapchat offers a variety of privacy settings that users are expected to alter to fit their inclinations and comfort level. For the most part, these settings are overtly simple to locate and can be turned on or off whenever users wish, should their perspective on any one aspect later change. In addition to its settings, Snapchat provides general protection updates that users have access to, such as notices about how to use Snapchat without unintentionally sending a private Snapchat to the wrong individual or posting something to their story that they initially intended to send privately. The usability of the privacy settings in Snapchat is moderately high given the ease of use.

Aljohani et al. [30] also mentioned the privacy settings in Snapchat, which, like an instant messenger, permits users to send photographs and drawings regardless of content. Pictures posted in a straightforward manner to companions vanish from Snapchat's servers after the assigned 24-hour timeframe lapses. In contrast to other networking platforms, Snapchat clients must add companions to have the option to collaborate, which demonstrates the usability of its privacy settings. If somebody unknown to a user attempts to send a snap, the user will be informed that he or she needs to include the sender as a companion. As already noted, users can modify Snapchat's privacy settings for enhanced security. The settings to adjust include the option of who can send snaps and who can see an account. Users can also select either "everybody" or "my friends only" for who will have access to the snaps they post. However, several privacy risks are associated with the use of such social media networks, which is the topic of the next section.

F. Privacy Risks in Social Media

Townsend and Wallace [31] reported that online users frequently post statuses about being out of town, visiting new locations, leaving their apartments with no one at home, and much more such information. Moreover, online users post photographs of themselves and share their complete names and birthdays, where they went to school, and where they work, all while seemingly unaware of the possibility that somebody could use that information to attempt to hurt them, find them, or impersonate them. A New York Times analytical report uncovered that an American organization named Devumi gathered millions of dollars in a shady worldwide commercial online fraud scheme. The company sold Twitter followers and retweets to individuals who hoped to become influencers on social media and increase their online popularity [32]. Devumi's customers were provided with millions of followers with profiles that could have been profiles of anyone but were certainly not profiles of actual people. This illustrates one of social media's privacy risks.

While there is proof that social networking platforms have been significant to individuals, Bergström [33] indicated that individuals are hesitant regarding issues concerning the personal data that are gathered and shared and the security of their information. For example, a 2014 review found that 91% of Americans concurred or unequivocally agreed that they had lost authority over how their private and personal data are gathered and used by a wide range of actors. In addition, a significant number of social media clients reported that they worried about businesses and organizations gaining access to the information they share on networking platforms. Based on these concerns, most online users supported the recommendation that governments be more involved in regulating promoters.

Baruh, Secinti, and Cemalcilar [34] noted that other surveys have revealed that social media platform users are not confident concerning their privacy settings in services such as Twitter, Snapchat, and WhatsApp. This is because most users are convinced that social media organizations are not capable of securing the information they share online. Even worse, Bergström [33] stated that users' concerns regarding privacy settings are founded on the fact that most users struggle to comprehend the nature and extent of the information gathered about them. Only a few social media users believe they have significant control over the data collected about them, which is certainly not always the case.

III. Methodology

A review of the available research methods for an evaluation study of the usability of privacy guided our decision to adopt the STRAP framework. Heuristic evaluation is a technique that is dependent on specific principles or rules ordinarily referred to as heuristics. Essentially, when performing a heuristic evaluation, a specialist evaluator uses guidelines for checking a compliance list to not only assess usability but also assign severity ratings to the heuristics [35]. Accordingly, in this type of evaluation, the heuristics incorporate a mixed combination of components, the greater part of which are derived from Nielsen's heuristics. This means that the principles and rules observed in heuristic evaluations can be derived either from explicit guidelines, practices, or hypotheses. In this way, proper heuristics offer designers the most effective corrective measures.

There are several advantages to this method that demonstrate why it is the most frequently chosen technique for usability analyses. More specifically, heuristic evaluations are not only fast but also intuitive, which allows them to provide feedback outcomes more quickly. In addition, they are moderately economical because time is conserved and assets are managed effectively [35]. Heuristic evaluations can also be joined with other ease-of-use testing strategies to more closely inspect potential ease-of-use issues. Using such a methodology prior to evaluator testing can reveal the quantity and seriousness of the design and development mistakes found by experts.

STRAP heuristics is a framework that is centered on user design and acts as a privacy awareness design tool. The objective of the STRAP framework is to address a portion of the investigations performed on privacy analysis systems. Accordingly, the STRAP framework joins components of heuristic evaluation and goal-focused analysis with an end goal of accomplishing viability while minimizing expenses [5]. A basic property of the STRAP framework is that it is not necessary for analysts to learn new skills or abilities. It is basically meant to support analysts by distinguishing privacy issues and the usability of systems. In turn, it is an add-on technique and is not used for addressing other components of design procedures. Table I shows the details of the STRAP heuristics.

TABLE I. STRAP Heuristics and Descriptions for Each

Heuristic		**Description**
1-Notice/Awareness	a. Available, accessible, and clear	Information about app activities is always available to users in a way that is simple to access and understand.
	b. Correct, complete, and consistent	Disclosure is complete, correct, and consistent in order for users to make informed decisions.
	c. Presented in context	Relevant information is presented for each transaction to minimize memory load and ensure users are aware of the consequence of their actions.
	d. Not overburdening	Disclosure takes into consideration human limitations in memory, ability, and interest. It provides succinct and relevant information.
2-Choice/Consent	a. Meaningful options	Whenever possible, users are given real options rather than opt-in/opt-out choices to avoid coercion and maximize benefits.
	b. Appropriate defaults	Privacy default settings reflect most users' concerns and expectations with regard to protecting their privacy.
	c. Explicit consent	The app avoids assuming consent whenever possible.
3-Integrity/Security	a. Awareness of security mechanisms	Users are provided with enough information to judge the security of the app and their information.
	b. Transparency of transactions	The app provides transparency in transactions and data use to build user confidence and trust.
4-Enforcement/ Redress	a. Access to own records	Users have access to all information the app has collected about them, regardless of source.
	b. Ability to revoke consent	Consent is retractable.

A. Justification for using the STRAP Framework

For investigating the usability of privacy in terms of HCI issues, relevant privacy frameworks are reviewed and can be broadly divided into two classifications:

1) Guidelines: The Fair Information Practices are a prime example of guidelines; they were early design guidelines designed to support data protection regulations and provide a system-centered viewpoint.

2) Process frameworks: Examples of process frameworks include the STRAP framework [35] and the question options criteria (QOC) process. These offer direction in terms of the evaluation and design of privacy-sensitive IT applications and have a user-centric emphasis.

The structured analysis of privacy (STRAP) framework puts forward 11 dedicated sets of privacy heuristics that are intended to be employed by designers to assess interactive systems. Based on usability heuristics and fair information procedures, the STRAP framework represents a structured method of evaluating nonfunctional user requirements (NFRs). There are two primary motivations as to why the STRAP heuristics are useful for this study. First, the approach is based on the notion that designers do not have a strong track record of paying sufficient attention to addressing social issues, such as privacy, when designing information systems. As such, they benefit from the utilization of a simple, lightweight application that can highlight social problems such as privacy. Second, heuristic evaluation approaches are affordable and valuable.

Additionally, the effectiveness and efficiency of the STRAP heuristics have been tested and evaluated by several researchers, such as Jamal and Cole [36] and Jensen [37], who have found that the tool represents a useful means of identifying security, privacy, and correlated usability problems. The explanation for picking the STRAP usability heuristics as opposed to others is that the STRAP heuristics indicate the weakness identified in privacy issues [5]. Jensen and Potts [35] stated that nonfunctional requirements are those related to the quality of a system. In that regard, the STRAP framework combines heuristics from other relevant frameworks, such as “GBRAM,” which makes it more effective as it builds on goal-oriented analytical approaches [38]. Gritzalis et al. [39] asserted that the STRAP framework proves to be more than effective when evaluating the privacy of systems. Regarding social media apps, the STRAP framework can be used to evaluate privacy based on whether they provide effective protection from privacy vulnerabilities. For instance, Gritzalis et al. [39] mentioned that the STRAP framework is effective because it combines elements of heuristic evaluation and elements of goal-oriented analysis, which not only minimizes expenses but also achieves better effectiveness. Moreover, for evaluating social media app privacy, the STRAP framework is justifiable because there is no need for analysts or evaluators to learn different or new skills. In these ways, the STRAP framework supports analysts in identifying privacy issues in social media apps.

B. Data Collection and Analysis

In this study, a STRAP heuristic evaluation was used to evaluate the usability of privacy for the WhatsApp, Twitter, and Snapchat apps. The reason for selecting three apps was to be able to make a reasonable comparison. In fact, the selection of these apps was based on their usage ranking and simplicity. For example, unlike Facebook, which has an unclear main purpose, Twitter is known for microblogging news, WhatsApp for instant messaging, and Snapchat for sharing personal stories.

Table II provides the specific versions of each app that were investigated. There were minor differences between the tested apps on Android and iOS. However, the authors ensured that these minor differences had no effect on the evaluation. In fact, some evaluators used Android, while the others used iOS.

TABLE II. THE INVESTIGATED VERSION OF EACH APP

App	Android	iOS
WhatsApp	2.20.157	2.20.51
Twitter	8.45.0-release.00	8.19
Snapchat	10.82.50	10.82.5.78

The authors of this study asked for the participation of eight faculty members in the departments of information technology and information systems in different universities near their area who had experience in this type of evaluation. The selection was based on the authors’ knowledge of who had the ability to perform this type of evaluation. One faculty member refused to perform the evaluation, claiming that there was no reward, while the others agreed. As stated by Nielson [5], heuristic analysis can be highly effective for general HCI problems by a small number of evaluators. In fact, Nielsen and Molich [40] recommended 3 to 5 evaluators to find most of the usability problems. However, we asked three more evaluators to ensure that we cover a larger number of usability problems.

Each evaluator performed the evaluation separately to avoid influencing each other. The evaluation process began with the expert evaluators applying the 11 STRAP heuristics (stated in Table I) to evaluate the privacy policy statements and settings provided by WhatsApp, Twitter, and Snapchat. All of the evaluators were given the same procedures to perform during the evaluation. For each privacy heuristic that was violated, the evaluator assigned one of the following severity ratings:

0 = I don’t agree that this is a usability problem at all

1 = Cosmetic problem only

2 = Minor usability problem

3 = Major usability problem

4 = Usability catastrophe

Seven expert evaluation lists were produced and then merged into one list by calculating the severity ratings for all of the survey statements for WhatsApp, Twitter, and Snapchat. For example, the number of evaluators for every severity rating for each heuristic for WhatsApp was counted, and then this number was multiplied by the severity rating to obtain the total (3); the totals are shown in Table III.

TABLE III. RESULTS OF THE STRAP HEURISTIC EVALUATIONS OF THE THREE APPS

Heuristic		**WhatsApp**	**Twitter**	**Snapchat**
1-Notice/Awareness	a. Available, accessible, and clear.	3	8	14
	b. Correct, complete, and consistent.	8	9	13
	c. Presented in context.	9	11	17
	d. Not overburdening.	8	6	10
2-Choice/Consent	a. Meaningful options.	12	14	18
	b. Appropriate defaults.	7	15	19
	c. Explicit consent.	17	10	14
3-Integrity/Security	a. Awareness of security mechanisms.	8	12	16
	b. Transparency of transactions.	11	11	16
4-Enforcement/ Redress	a. Access to own records.	19	9	10
	b. Ability to revoke consent.	17	17	20
Total		116	122	167

IV. RESULTS AND DISCUSSION

The severity ratings of the usability problems regarding privacy issues in each app are presented in Table III. This table includes both the ratings for each heuristic individually and the ratings for all heuristics added together. The description of each heuristic was previously provided in Table I. Table III reveals that, overall, Snapchat had the highest severity rating (167), which was much higher than the ratings for WhatsApp (116) and Twitter (122). It shows the total severity rating for each app based on the five scales of the severity rating. As shown in Table III, the severity rating for Snapchat exceeded the score for minor usability problems.

Snapchat consistently had the highest rating for each separate heuristic except for meaningful options and access to the user's own records, where WhatsApp had the highest ratings. In the rest of the heuristics, Twitter had higher usability problem ratings than WhatsApp, except in three heuristics. In the heuristic "not overburdening," WhatsApp had a higher rating (8) than Twitter (6). In the heuristics of "transparency of transactions" and "ability to revoke consent," the apps had the same ratings (11 and 17, respectively). In fact, when the five scales of the severity rating are applied to one heuristic individually, the maximum score is as follows:

Catastrophic = 28

Major = 21

Minor = 14

Cosmetic = 7

None = 0

By looking at the severity rating for each heuristic separately, WhatsApp had the lowest rating (3) with regard to the availability, accessibility, and clarity of privacy notices. Twitter's rating (8) was notably higher than WhatsApp's rating, while Snapchat's rating (14) was the highest. This result is not surprising given that Snapchat suffers from various issues that belong to this heuristic. Snapchat confuses users by mixing certain information together and making several settings difficult to understand. For example, Snapchat has a section called "additional services" that contains several privacy settings, and under that section, there is another section called "privacy," as shown in Fig. 1. Additionally, Snapchat takes users away from the settings screen when they do not interact with the app for a few moments, which makes it difficult for users to return to where they left off.

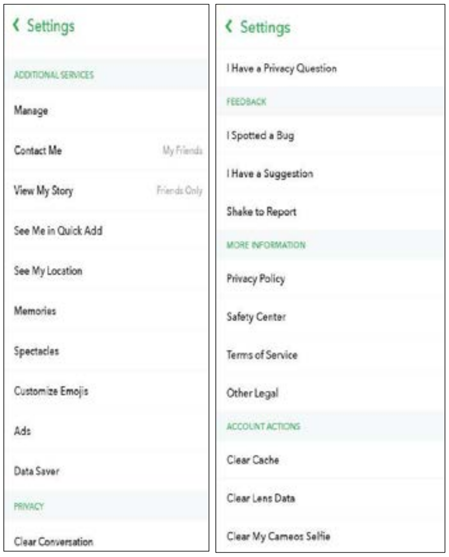


Fig. 1. Privacy Settings in Snapchat.

In contrast, WhatsApp has all its privacy settings in one location (i.e., under "privacy"). Furthermore, this section is displayed with a lock sign, which gives users a hint about the types of settings in that section. Moreover, this section is contained under "account," which is designated with a key symbol, as shown in Fig. 2. Additionally, the privacy policies are listed under "help," which is denoted by a question mark sign. Using icons reduces the mental load for users and allows for smooth navigation [41], [42]. Thus, the privacy settings and policies look organized and clear in WhatsApp. In Twitter, the privacy settings also look organized; however, it is not clear how to find the privacy policies. It is important to mention that the interface of the privacy settings may look slightly different in the two operating systems that were investigated (Android and iOS). However, the analysis is still valid for both. Regarding the second heuristic (Table III, 2a), which measures the completeness, correctness, and consistency of a disclosure, the severity rating was similar for WhatsApp (8) and Twitter (9) but was notably higher for Snapchat (13).

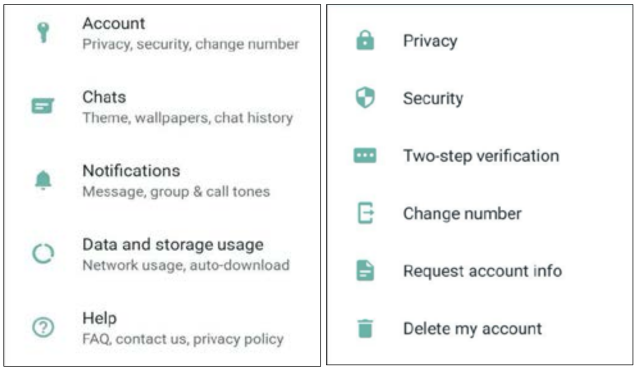
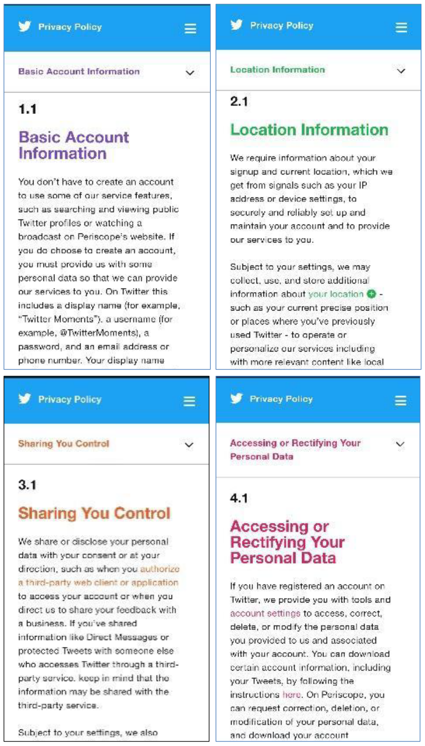

Account
Privacy, security, change number
Chats
Theme, wallpapers, chat history
Notifications
Message, group & call tones
Data and storage usage
Network usage, auto-download
Help
FAQ, contact us, privacy policy
Privacy
Security
Two-step verification
Change number
Request account info
Delete my account

Fig. 2. Privacy Settings in WhatsApp.

The fourth heuristic (Table III, 4a), measuring whether a disclosure is overburdening, resulted in a slightly lower severity rating for Twitter (6) than for WhatsApp (8) or Snapchat (10). It is not surprising to see that Twitter's rating is the lowest here. One reason is that Twitter divides its privacy policies into sections, each of which is color coded, as shown in Fig. 3. The colors make it easy for humans to link information to the right section. In fact, some scholars have indicated that "color in user interface can control the user's attention, help to recognize interface elements, express the meaning of indicators in complex professional systems, as well as be used for visual grouping of similar objects" [43].



1.1

Basic Account Information

You don't have to create an account to use some of our service features, such as searching and viewing public Twitter profiles or watching a broadcast on Periscope's website. If you do choose to create an account, you must provide us with some personal data so that we can provide our services to you. On Twitter this includes a display name (for example, "Twitter Moments"), a username (for example, @TwitterMoments), a password, and an email address or phone number. Your display name

2.1

Location Information

We require information about your signup and current location, which we get from signals such as your IP address or device settings, to securely and reliably set up and maintain your account and to provide our services to you.

Subject to your settings, we may collect, use, and store additional information about your location - such as your current precise position or places where you've previously used Twitter - to operate or personalize our services including with more relevant content like local

3.1

Sharing You Control

We share or disclose your personal data with your consent or at your direction, such as when you authorize a third-party web client or application to access your account or when you direct us to share your feedback with a business. If you've shared information like Direct Messages or protected Tweets with someone else who accesses Twitter through a third-party service, keep in mind that the information may be shared with the third-party service.

Subject to your settings, we also

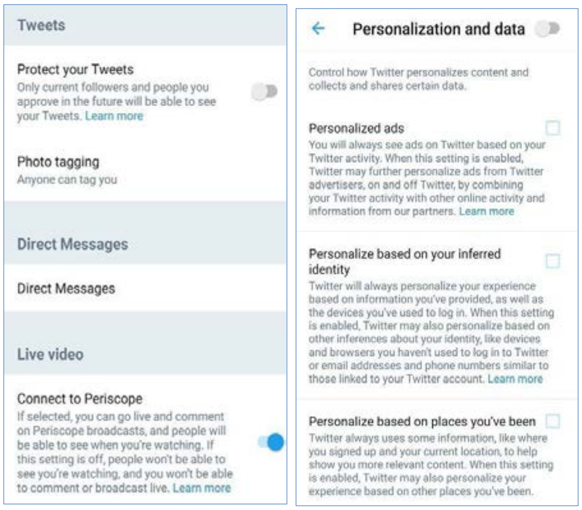
4.1

Accessing or Rectifying Your Personal Data

If you have registered an account on Twitter, we provide you with tools and account settings to access, correct, delete, or modify the personal data you provided to us and associated with your account. You can download certain account information, including your Tweets, by following the instructions here. On Periscope, you can request correction, deletion, or modification of your personal data, and download your account

Fig. 3. Privacy policies on Twitter.

The third heuristic, which measures the presentation of relevant information that belongs to each transaction, revealed that the highest severity rating was given to Snapchat (17). Twitter's rating (11) for this heuristic was closer to that of WhatsApp (9). Generally, Twitter provides a short explanation for each setting and a link to "learn more," as shown in Fig. 4. Conversely, while neither Snapchat nor WhatsApp provides a link to additional explanations for each setting, WhatsApp performs slightly better because it does not have jargon that could result in some users being unaware of the consequences of certain actions. For instance, Snapchat has the setting "clear top locations," which is used for "Map Actionmoji." However, there is inadequate information provided about this jargon and the consequences of the setting.



Protect your Tweets
Only current followers and people you approve in the future will be able to see your Tweets. Learn more

Photo tagging
Anyone can tag you

Connect to Periscope
If selected, you can go live and comment on Periscope broadcasts, and people will be able to see when you're watching. If this setting is off, people won't be able to see you're watching, and you won't be able to comment or broadcast live. Learn more

Control how Twitter personalizes content and collects and shares certain data.

Personalized ads □
You will always see ads on Twitter based on your Twitter activity. When this setting is enabled, Twitter may further personalize ads from Twitter advertisers, on and off Twitter, by combining your Twitter activity with other online activity and information from our partners. Learn more

Personalize based on your inferred identity □
Twitter will always personalize your experience based on information you've provided, as well as the devices you've used to log in. When this setting is enabled, Twitter may also personalize based on other inferences about your identity, like devices and browsers you haven't used to log in to Twitter or email addresses and phone numbers similar to those linked to your Twitter account. Learn more

Personalize based on places you've been □
Twitter always uses some information, like where you signed up and your current location, to help show you more relevant content. When this setting is enabled, Twitter may also personalize your experience based on other places you've been.

Fig. 4. Privacy Settings on Twitter.

Generally, the heuristics evaluating "choice and consent" revealed more usability problems than the heuristics evaluating "notice and awareness." In the second group of heuristics, evaluating whether apps provide meaningful options, all the apps had high severity ratings. Specifically, the rating was 12 for WhatsApp, 14 for Twitter, and 18 for Snapchat. In other words, users are given the choice to opt in or opt out rather than more specific options for most privacy issues. The next heuristic in this group, which evaluated whether the apps had appropriate defaults, resulted in a significant difference between WhatsApp and the other apps. WhatsApp's rating (7) was less than half the ratings for Twitter (15) and Snapchat (19). WhatsApp still does not allow banner ads as Twitter and Snapchat do, which is one reason for the lower rating for WhatsApp. Additionally, Twitter and Snapchat normally allow interaction with unknown people more than WhatsApp does.

Moreover, because Twitter and Snapchat sell ad space, they prefer that users select the default settings, which maximize their benefits. Snapchat has the highest score here because it is basically about sharing a personal story and, thus, it is about sharing very sensitive information. In marked contrast, WhatsApp's rating for avoiding an assumption of consent whenever possible was the highest (17) compared to Twitter (10) and Snapchat (14). An example that could explain why WhatsApp had the highest rating here is the fact that users have no choice about whether to share their private information with

Facebook. Overall, usability problems were high for all the apps under this heuristic. One reason for the usability problems is that the apps share users' private information with third parties whether the users agree or not.

The evaluation of the awareness of security mechanisms and transparency of transactions shows that Snapchat had the most usability problems overall. One reason for this evaluation is that Twitter and WhatsApp explain why they collect data in several cases, unlike Snapchat. WhatsApp and Twitter also provide specific explanations of the data they collect, while Snapchat provides general explanations to encompass all the data it collects. However, all the apps need to provide more convincing details about how users' data are being used and how users are protected. In Twitter, several settings cannot be controlled solely through a user's Twitter account. Users are therefore asked to opt out of other organizations' services to attain certain privacy goals. This is commonly seen with settings related to ads. For example, users are encouraged to opt out of Google Analytics by installing Google's opt-out browser add-on and to opt out of interest-based Google ads using Google's Ads Settings.

In the last group of heuristics, evaluating users' ability to access their own records, WhatsApp had the worst severity rating (19). In fact, WhatsApp does not provide a clear way for users to access their own records. Conversely, Twitter and Snapchat clearly show that feature in their privacy settings. Because not all records are accessible, usability issues still existed for this heuristic. The results related to the last heuristic, measuring the ability to revoke consent, are the most notable because all the apps had a dramatically higher number of usability problems. In other words, there is no option to revoke the user agreement in any of these apps. In Twitter, consent is revocable for several settings but only with certain conditions. In other words, changes may not occur immediately or may not be applied in certain cases. For example, when users change the setting for their tweets from public to protected, there is no guarantee that no past tweets will be shown in search engine results.

V. Recommendation

Based on the analytical results of the current study, we can say that the way privacy settings and privacy policies are presented needs to be reconsidered. The tested apps present their privacy settings and privacy policies differently, which makes using them difficult. For example, WhatsApp places its privacy policies under "Help", Twitter under "About Twitter", and Snapchat under "More Information". The current presentation or mapping works against one of the core principles of usability (i.e., consistency). Thus, it is recommended that these apps make privacy a main section that includes both their privacy settings and their privacy policies.

Another recommendation is about the need to attach interactive visual signs to the text that describes the privacy settings and policies. Furthermore, assigning different colors for different settings and policies helps users recognize the differences between them and increases their learnability toward the usage of the settings and policies.

VI. Conclusion

This paper presented a heuristic evaluation of the usability of privacy in WhatsApp, Twitter, and Snapchat based on the STRAP framework. It highlighted useful information for designers and developers of social media applications as well as users of the apps to enhance the usability of privacy. The results of the study pointed out several privacy issues in each of the investigated apps. It further indicated that Snapchat had many more usability problems than WhatsApp and Twitter, which had relatively close scores regarding usability problems. In terms of evaluating each heuristic individually, the most notable severity rating for all the apps was on the ability to revoke consent, where all the apps had a very high number of usability problems. Overall, careful consideration needs to be given to the issues discussed in this paper to enhance the usability of privacy in these social media apps. Finally, it is suggested that future research should consider how to increase users' awareness to protect their information on social media networks.

Acknowledgment

The authors acknowledge the deanship of scientific research at King Faisal University for the financial support under Ra'ed Track (Grant No. 207005). The authors also acknowledge the participation of the seven expert evaluators who performed the heuristic evaluation in this study.

References

[1] Statista. "Social media: global penetration rate 2020, by region," https://www.statista.com/statistics/269615/social-network-penetration-by-region.

[2] M. Bedjaoui, N. Elouali, and S. M. Benslimane, "User time spent between persuasiveness and usability of social networking mobile applications: a case study of Facebook and YouTube," in Proc. of the 16th International Conference on Advances in Mobile Computing and Multimedia, pp. 15–24, November 2018.

[3] T. Paul, D. Puscher, and T. Strufe, "Improving the usability of privacy settings in Facebook." arXiv preprint arXiv:1109.6046, 2011.

[4] A. Albesher and T. Alhussain, "Privacy and security issues in social networks: an evaluation of Facebook," in Proc of the 2013 International Conference on Information Systems and Design of Communication, pp. 7–10, July 2013.

[5] C. Jensen, J. Tullio, C. Potts, and E. D. Mynatt. "STRAP: A structured analysis framework for privacy." Georgia Institute of Technology, 2005.

[6] A. L. Langhorne, "Web privacy policies in higher education: How are content and design used to provide notice (or a lack thereof) to users?" in International Conference on Human Aspects of Information Security, Privacy, and Trust, pp. 422–432, June 2014.

[7] E. Schwartz, "Exploring Experience Design: Fusing Business, Tech, and Design to Shape Customer Engagement", Packt Publishing Ltd., Birmingham, UK, 2017.

[8] K. D. Martin and Murphy, P. E. "The role of data privacy in marketing," Journal of the Academy of Marketing Science, vol. 45, no. 2, 135-155, 2017.

[9] S. Warren and L. Brandeis., "The Right to Privacy," Harvard law review, vol. 4, no. 5, 193-220, December, 1890.

[10] C. L. Miltgen and H. J. Smith, "Exploring information privacy regulation, risks, trust, and behavior," Information & Management, vol. 52, no. 6, pp. 741–759, September 2015.

[11] H. Choi, J. Park, and Y. Jung, "The role of privacy fatigue in online privacy behavior." Computers in Human Behavior, vol. 81, pp. 42–51, April 2018.

[12] C. Bunnig and C.H., Cap, "Ad hoc Privacy management in ubiquitous computing environments," In CENTRIC '09., September 2009, pp.85-90.

[13] N. Aldhafferi, C. Watson, and A. S. Sajeev, “Personal information privacy settings of online social networks and their suitability for mobile internet devices.” International Journal of Security, Privacy and Trust Management, vol. 2, no. 2, pp. 1–17, 2013.

[14] L. Kagal and H. Abelson, “Access control is an inadequate framework for privacy protection,” in W3C Privacy Workshop, pp. 1–6, July 2010.

[15] T. Trojer, B. Katt, T. Schabetsberger, R. Breu, and R. Mair, “Considering privacy and effectiveness of authorization policies for shared electronic health records,” in Proc. of the 2nd ACM SIGHIT, pp. 553–562, January 2012.

[16] D. G. Krone, “Facebook and user-controlled privacy: evaluating privacy settings as notice-and-consent.” Master’s thesis, Georgetown University, 2012.

[17] C. G. Akcora and E. Ferrari, “Graphical user interfaces for privacy settings,” in Encyclopedia of Social Network Analysis and Mining, R. Alhajj and J. Rokne (eds.), Springer, New York, NY, 2018.

[18] G. C. Kane, “Enterprise social media: current capabilities and future possibilities.” MIS Quarterly Executive, vol. 14, no. 1, 2015.

[19] D. Trottier, Social Media as Surveillance: Rethinking Visibility in A Converging World, reprint ed., Routledge, 2016.

[20] H. Quay-de la Vallee, J. M. Walsh, W. Zimrin, K. Fisler, and S. Krishnamurthi, “Usable security as a static-analysis problem: modeling and reasoning about user permissions in social-sharing systems,” in Proc. of the 2013 ACM International Symposium on New Ideas, New Paradigms, and Reflections on Programming & Software, pp. 1–16, October 2013.

[21] F. Alt and E. V. Zezschwitz, “Emerging Trends in Usable Security and Privacy,” Journal of Interactive Media, vol. 18, no. 3, pp. 189–195, 2019.

[22] F. Schaub and L. F. Cranor, “Usable and Useful Privacy Interfaces,” in An introduction to privacy for technology professionals, Portsmouth, NH: International Association of Privacy Professionals, pp. 176–229, 2020.

[23] P. Raschke, A. Küpper, O. Drozd, and S. Kirrane, “Designing a GDPR-Compliant and Usable Privacy Dashboard,” IFIP Advances in Information and Communication Technology Privacy and Identity Management. The Smart Revolution, pp. 221–236, 2018.

[24] N. Sadeh, A. Acquisti, T.D. Breaux, L.F. Cranor, A.M. McDonald, J. Reidenberg, N.A. Smith, F. Liu, N.C. Russell, F. Schaub, and S. Wilson, "The Usable Privacy Policy Project: Combining Crowdsourcing, Machine Learning and Natural Language Processing to Semi-Automatically Answer Those Privacy Questions Users Care About.", Tech. report CMU-ISR, Dec. 2013, 13-119.

[25] J. Angulo, S. Fischer-Hübner, E. Wästlund, and T. Pulls, “Towards usable privacy policy display and management”, In Information Management & Computer Security, March, 2012, pp.4-17.

[26] R. Jones, N. Sailaja, and L. Kerlin, “Probing the Design Space of Usable Privacy Policies: A Qualitative Exploration of a Reimagined Privacy Policy,” Electronic Visualisation and the Arts, pp. 1–12, 2017.

[27] C. Fiesler, et al. “What (or who) is public? Privacy settings and social media content sharing,” in Proc of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, pp. 567–580, February 25–March 1, 2017.

[28] J. Dev, S. Das, and L. J. Camp, “Privacy practices, preferences, and compunctions: WhatsApp users in India,” in Proc. of the 12th International Symposium on Human Aspects of Information Security & Assurance, pp. 135–146, 2018.

[29] M. Mondal, G. S. Yilmaz, N. Hirsch, et al. “Moving beyond set-it-and-forget-it privacy settings on social media,” in Proc. of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 991–1008, November 2019.

[30] M. Aljohani, A. Nisbet, and K. Blincoe, “A survey of social media user’s privacy settings & information disclosure,” in Proc. of 14th Australian Information Security Management Conference, pp. 67–75, December 5–6, 2016.

[31] L. Townsend and C. Wallace, “Social media research: a guide to ethics.” University of Aberdeen, pp. 1–16, 2016.

[32] N. Confessore, G. J. Dance, R. Harris, and M. Hansen, “The follower factory.” The New York Times, January 27, 2018.

[33] A. Bergström, “Online privacy concerns: a broad approach to understanding the concerns of different groups for different uses.” Computers in Human Behavior, vol. 53, pp. 419–426, July 2015.

[34] L. Baruh, E. Secinti, and Z. Cemalcilar, “Online privacy concerns and privacy management: a meta-analytical review.” Journal of Communication, vol. 67, no. 1, pp. 26–53, February 2017.

[35] C. Jensen and C. Potts. “Experimental evaluation of a lightweight method for augmenting requirements analysis,” in Proc. of the 1st ACM International Workshop on Empirical Assessment of Software Engineering Languages and Technologies: Held in Conjunction With the 22nd IEEE/ACM International Conference on Automated Software Engineering, pp. 49–54, 2007.

[36] A. Jamal and M. Cole, “A Heuristic Evaluation of the Facebook's Advertising Tool Beacon”, First International Conference on Information Science and Engineering, pp.1527-1530, 2009.

[37] C. Jensen, ‘‘Toward a method for privacy vulnerability Analysis’’, CHI 2004, extended abstracts on Human factors in computing systems, Publisher: ACM 2004.

[38] A. Antón, and J. Earp, “Strategies for developing policies and requirements for secure electronic commerce system,” in Proc. of the 1st Workshop on Security and Privacy in E-Commerce, pp. 67-86, Springer, Boston, MA, 2009.

[39] S. Gritzalis, E. R. Weippl, S. K. Katsikas, G. Kotsis, A. M. Tjoa, and I. Khalil (eds.), “Trust, Privacy, and Security in Digital Business,” 16th International Conference, TrustBus 2019, August 26–29, 2019.

[40] J. Nielsen, J., and R. Molich, “Heuristic evaluation of user interfaces,” In Proceedings of the SIGCHI conference on Human factors in computing systems, March 1990, pp. 249-256.

[41] C. F. Li, H. T. Shi, J. J. Huang, and L. Y. Chen, “Two typical symbols in human-machine interactive interface,” Applied Mechanics and Materials, vol. 635, pp. 1659–1665, 2014.

[42] B. Merdenyan, O. Kocyigit, R. Bidar, O. Cikrikcili, and Y. B. Salman, “Icon and user interface design for mobile banking applications,” in ACIT’14, June 2014.

[43] A. Mandrik, L. Sopronenko, N. Rushchenko, and A. Lavrov, “User interface design based on color schemes of paintings’ digital reproductions,” in Proc. of the 11th Majorov International Conference on Software Engineering and Computer Systems, paper 27, December 12–13, 2019.