


Evaluating Cognitive Privacy Heuristics that Influence Facebook Users Data Disclosure

Daphne Fernanda F. B. de Carvalho   [Pontifical Catholic University of Minas Gerais | daphne.bueno@sga.pucminas.br]

Cristiane N. Nobre  [Pontifical Catholic University of Minas Gerais | nobre@pucminas.br]

Humberto T. Marques-Neto  [Pontifical Catholic University of Minas Gerais | humberto@pucminas.br]

 Pontifical Catholic University of Minas Gerais - PUC Minas - 500 Dom José Gaspar Street, Building 20, Coração Eucarístico, Belo Horizonte, MG 30535-901, Brazil

Received: 04 March 2022 • **Accepted:** 11 July 2022 • **Published:** 16 December 2022

Abstract Privacy protection has been a challenging issue in online social networks, such as Facebook, Instagram, and Snapchat. The General Data Protection Regulation (GDPR), which protects the privacy and security of individuals, entered into force on May, 2018. This regulation intends to enhance individuals' control and rights over their own data, guided by lawfulness, loyalty, transparency, adequacy, purpose limitation, need, or minimization. However, despite regulatory efforts to protect personal data online, users are prone to consent to disclose more personal information than they intend and tend to reveal more than they know. With this in mind, the main goal of this study is to carry out a heuristic evaluation of the online social network Facebook to identify the factors that influence the disclosure of user information and verify informed consent. For this, we carried out a survey of cognitive heuristics that influence individuals' decisions to protect or renounce their privacy. Then, using these heuristics, we conducted a heuristic evaluation on Facebook to explore a significant presence of cue triggers for a specific cognitive heuristic that helps users make their decisions. We found on Facebook a notable amount of heuristics that increase information disclosure, such as modality and narrative. However, the intrusiveness heuristic was also detected, violating the Privacy by Design (PbD) principle of "Privacy as the Default Setting". Accordingly, understanding the number and diversity of suggestions (heuristics) to which users are susceptible allows the creation of explicit guidelines addressing privacy concerns.

Keywords: Privacy, Cognitive heuristics, Information disclosure, Informed consent, Heuristic evaluation, Online Social Network, Facebook

1 Introduction

The privacy of the information handled by systems is often regarded as a matter of concern. Before the Internet, users' activities were traditionally private or shared with few people, but now they leave traces of their interests, characteristics, beliefs, and intentions. According to Acquisti *et al.* [2015], information is revealed by people – intentionally and involuntarily – with each other, commercial entities, and government. Therefore, the breach of privacy can threaten an individual's autonomy as a consumer and citizen. Furthermore, Acquisti *et al.* [2015] stated that information sharing does not always result in increased efficiency, progress, or equality.

With the growth of personal concerns about ensuring privacy when using different applications, such as mobile applications and online services, several countries have signed new laws that regulate the issue of collection, storage, treatment, and sharing of personal data. On May 25, 2018, the General Data Protection Regulation (GDPR) was implemented in Europe. As part of GDPR, digital privacy is guaranteed by a set of principles, including lawfulness, loyalty, transparency, adequacy, restriction of purposes, minimization, data quality, accuracy, conservation limits, security, integrity, confidentiality, and accountability. In Brazil, the

General Data Protection Law (LGPD) was approved on August 14, 2018, and the text entered into force on September 18, 2020. GDPR is the utmost influence on the creation and maturation of the LGPD. The LGPD alters articles from Marco Civil da Internet and establishes new rules for companies and public organizations concerning the treatment of privacy and security of user and customer information. The LGPD articles on administrative sanctions for those who break the rules on personal data processing came into effect on August 1, 2021. Punishments can reach up to 2% of revenues up to the limit of 50 million Reais [Lei N° 14.010, 2020].

On the other hand, the advent of the Internet and technological advances has given rise to Online Social Networks (OSNs), which are now the primary means of connecting to the Internet for millions of people. OSNs enable users to share information with friends and facilitate interpersonal communication and interaction. However, users' most significant risk when joining a social network is controlling data about themselves [Baden *et al.*, 2009; Rodrigues *et al.*, 2017]. As reported by Estivill-Castro and Nettleton [2015], social networks provide users with many benefits, including virtual socialization, wide transmission, collaboration, and communication. Nevertheless, they cannot regulate the restriction of the circles in which data is shared. The degree to which

they control their data is, however, one of the most common privacy measures.

It has been well documented and confirmed by several authors that the dispositions of others may influence users' privacy decisions. Examples include Gambino *et al.* [2016]; Vincent *et al.* [2017]; Wu *et al.* [2018]. According to Wu *et al.* [2018], users' disclosure behaviors are likely influenced by several heuristics. For instance, the disclosure of information already disclosed by others, withholding information when an item is unexpectedly ordered, or using social media default privacy settings. The application of heuristics is an effective method for solving problems rapidly and making accurate judgments.

By relying on rule-of-thumb (heuristics) strategies, people are able to perform better, as they will not be compelled to constantly think about their next move. Sundar *et al.* [2020] declared that heuristics are not invented at the interaction but represent stable associations formed in the user's mind. According to the authors, a determining factor to trigger a heuristic when using an interface is the degree of accessibility of that heuristic in the individual's mind.

Per the large number of users in OSNs, our study opts to inspect Facebook, which is the 3rd most visited website in the world. It is second only to Google and YouTube. Facebook had over 2.9 billion monthly active users (MAU) and 1.93 billion (66% of MAUs) daily active users (DAUs) at the end of the third quarter of 2021. On average, Facebook users spend 34 minutes per day on the site. 53% of users do not understand how their newsfeed is displayed. It is expected that Facebook's ad revenues will reach 94.69 billion dollars in 2021 [Statista, 2021; Social Media Perth, 2021; Omnicore, 2021].

The main goal of this study is to carry out a heuristic evaluation of the online social network Facebook to identify the factors that influence the disclosure of user information and verify informed consent. For this, we carried out a survey of cognitive heuristics that influence individuals' decisions to protect or renounce their privacy.

Heuristic evaluation is one of the existing methods for usability inspection, which involves a team of individuals examining how an interface is designed following usability guidelines at a low cost [Nielsen, 1994]. In this work, three specialists worked on the evaluation, two of them with experience in Characterizing and Modeling Online Social Network User Behavior, including Privacy and Information Security issues, and the other with large experience in the area of Human-Computer Interaction, especially in the areas of Usability and Accessibility. We analyzed, among the most accessed features on Facebook, those heuristics that favor the increase or inhibition of information disclosure.

Thus, the study carried out and presented in this article unfold privacy heuristics, that supports (or not) compliance with the transparency pillar established in the data protection laws. In this study, we examine a set of privacy heuristics that affect individuals' decisions about disclosing information. For example, after completing a heuristic evaluation regarding the social network Facebook, it was possible to ascertain that most of the heuristics identified in the literature can be acting as a factor for increasing users' disclosure. Accordingly, understanding the number and diversity of sug-

gestions (heuristics) to which users are susceptible allows the creation of explicit guidelines addressing privacy concerns and to envision the application of Privacy by Design (PbD), incorporating privacy protection at the core of all product development.

The remainder of this paper is organized as follows. In Section 2, we present a theoretical framework outlining the definition of privacy, the privacy paradox, GDPR and LGPD laws, consent of the data subject, and the seven principles for Privacy by Design (PbD). Afterward, Section 3 describes the methodology used to uncover cognitive privacy heuristics on the social network Facebook. The results of the heuristic analysis and a discussion of the results are provided in Section 4. At last, Section 5 shows this work's final considerations.

2 Theoretical Framework

This section explains the definition of privacy, the privacy paradox, GDPR (European countries) and LGPD (Brazil) laws, the consent of the data subject, as well as seven principles for Privacy by Design (PbD).

2.1 Privacy

Contemporary attention is focused on the concept of information privacy, which contains several different conceptualizations of privacy. As pointed out by Solove [2006], privacy was also interpreted as territorial and physical, encompassing concepts such as surveillance, protection, dignity, intrusion, exposure, insecurity, secrecy, anonymity, appropriation, and as well as freedom.

Altman [1975] in his analysis of privacy emphasizes multiple levels (individual and group) of analysis, behavior (i.e. privacy regulation mechanisms) operating in a unified way as a coherent system, and a temporal (i.e. dynamic) and dialectical perspective on the regulation of privacy (i.e. over time the person or group, in response to changing conditions, opens and closes the self or group to others). His theory of privacy also reflects his commitment to social and environmental psychology because social interaction is at the heart of his theory and because the environment provides mechanisms to regulate privacy. Thus, according to Altman, social interactions, the social and physical environment and the cultural context are considered fundamental characteristics to understand the different properties of privacy and the multiple behavioral mechanisms (which might include environmental, verbal, non-verbal, or cultural aspects) for its regulation. In general terms, we can conclude that Altman emphasizes social interaction, which leads to a more inclusive conception of privacy.

Westin [2003], like Altman [1975], has influenced how researchers understand privacy. Westin [2003] defined privacy "as an individual's claim to determine what information about himself should be known to others". Besides, the author states that it is relevant to consider the use and circumstances for which other users obtain this information. The author argues that privacy in a society can be addressed at three levels: the *political* level, the *sociocultural* level, as

well as the *individual* level. At the *political* level, every society based on its political philosophy establishes a distinct balance between the private sphere and public order. At the *sociocultural* level, the constant observation of other people by others is shaped by the various environmental factors, such as the size and composition of urban areas, wealth class, and race [Westin, 2003].

Privacy at the *individual* level focuses on the individual and his daily experience when interacting directly with other people, being a function of family life, education, social class, and psychological composition. This privacy dimension reflects each individual's needs and desires and the progress of the life cycle and prevailing conditions. Westin [2003] pointed out that, there are four psychological conditions or states of personal privacy: loneliness, intimacy, anonymity, and reserve.

According to empirical and theoretical research, users are generally under-informed before making privacy-sensitive decisions. In exchange for short-term benefits, however, users are likely to trade their privacy. There are many different ways in which people disclose their personal information, and a single strategy does not work for everyone. For example, Wu *et al.* [2018] states that each user has specific privacy preferences for particular items. It is mentioned in Estivill-Castro and Nettleton [2015]; Neumann *et al.* [2019] that each user has a degree of confidentiality associated with the availability of each item of information.

Ataei *et al.* [2018] claim privacy is problematic since several factors and dimensions vary according to culture or context. Like Wu *et al.* [2018], the authors consider that the perception of privacy can also be subjective and differ from one individual to another. Therefore, it makes sense for designers or developers to carefully select the most appropriate definition according to the developed system's purpose.

2.2 Privacy Paradox

Discrepancies between the attitudes and behaviors of individuals are known as the privacy paradox, as a result of the diverging attitudes. There may be a desire to protect privacy in general, but depending on the costs and benefits of a particular situation, one may decide not to do so. Calculating costs and benefits rationally is only one part of how privacy decisions are made. A further factor influencing decision making is the misperception of costs and benefits, social norms, emotions, and heuristics.

According to Acquisti *et al.* [2015], incomplete and asymmetric information is the root cause of privacy uncertainty. According to the authors, individuals rarely have a clear understanding of what information third parties, companies, and governments have about them, how this information is used, or to what end this is done. While some damage to privacy is tangible, such as the financial costs associated with identity theft, many other injuries are intangible, such as strangers who become aware of someone's life story [Acquisti *et al.*, 2015].

Acquisti *et al.* [2015] states that individuals who lack a clear understanding of their preferences usually examine their surroundings to provide guidance. In terms of privacy, context can be understood as the degree to which an individ-

ual displays extreme concern or apathy regarding their privacy, depending on the situation.

Regarding privacy, stated intentions do not necessarily reflect individuals' behavior since independent factors, such as heuristic processing and habituation, influence choice and behavior. By creating a trusting relationship with consumers, Norberg *et al.* [2007] argues that organizations can considerably decrease privacy concerns.

According to Oliveira *et al.* [2021], people who use applications have a subjective relationship between "perceived advantage" and "perceived risks". According to the authors, when this relationship is positive, it leads to a more open-minded attitude toward technology, even when there are concerns about security. The cost-benefit ratio for mobile devices, according to the authors, is even more delicate as mobile devices can collect sensitive data continuously. Accordingly, the popularity of social networks and online shopping apps can be viewed as the privacy paradox, as sensitive information may be collected or exposed.

According to Kokolakis [2017], there are significant implications for e-commerce, e-government, online social networking, and government privacy regulation in relation to the privacy paradox. A large amount of personal information is collected by e-commerce and social networking sites. The author affirms that the essential aspect of the paradox, is the fact that often privacy intentions do not lead to protective behaviour. Wu [2018] argues that in the context of online social networking, "privacy paradox" may not be a paradox per se. Rather, privacy concerns reflect the ideology of an autonomous self, while self-disclosure answers one's need to be recognized by others.

Young and Quan-Haase [2013] affirms that an improved understanding of the privacy paradox has implications for design. The development of privacy policies that more closely mirror the needs and practices of users can be informed by assessing how they protect themselves in order to develop privacy controls that more closely reflect those strategies.

2.3 GDPR (General Data Protection Regulation) and LGPD (General Data Protection Law)

The General Data Protection Regulation (GDPR) has dramatically changed the landscape of data protection and the right to privacy of individuals. One of the topics covered by the GDPR is explicit consent. The user must confirm their consent to the sharing of Personally Identifiable Information (PII) before an organization can store this data. GDPR expands the definition of PII far beyond the name, address, and date of birth, encompassing the user's location (including IP address), health, genetic data (including biometric data), sexual orientation, race, ethnicity, religious beliefs, or political opinions. In addition, GDPR regulates users' rights, it expands the rights of individuals in relation to accessing and moving their own data, which stand out the right to delete and the right to be forgotten [GDPR, 2019].

In the GDPR law, Article 5 presents seven principles relating to processing users personal data, which describes:

1. **Lawfulness, fairness and transparency:** subject's

data is processed lawfully, fairly, and transparently.

2. **Purpose limitation:** specifically collected for explicit, legitimate purposes and not further processed in a way that conflicts with those purposes.
3. **Data minimisation:** the data must be adequate, relevant, and restricted to what is necessary for the purposes for which they are processed.
4. **Accuracy:** personal data must be accurate and, if necessary, kept up to date; steps must be taken to ensure that inaccurate personal data is erased or recycled.
5. **Storage limitation:** the personal data of subjects will only be kept as long as necessary to meet the purposes for which they were collected. To safeguard the rights and freedoms of data subjects, GDPR requires the implementation of appropriate technical and organisational measures.
6. **Integrity and confidentiality:** personal data is processed in a way that ensures appropriate security, including protection from unauthorised or unlawful processing, accidental loss, destruction, or damage
7. **Accountability:** controllers are responsible for ensuring compliance and must demonstrate compliance to previous principles.

As pillars of the General Data Protection Law (LGPD), there is transparency, management, and governance. It establishes rules for collecting, storing, treating, and sharing personal data, imposing more protection and penalties for its non-compliance [LGPD Brasil, 2019]. Regarding the pillar of transparency (Article 6 - VI), law No. 13.709 defines a guarantee to the holders of data about clear, accurate, and easily accessible information on data processing performance and the respective processing agents' of personal data. Another issue dealt with in the new law is the data subject's consent (Article 5 - XII), with a concept similar to the definition mentioned in GDPR [Lei N° 13.709, 2018].

LGPD also describes 10 principles in Article 6. They are similar to the principles described in GDPR. For example, the principle of "Purpose limitation" in GDPR are similar to the principles of "Purpose" and "Adequacy" in LGPD – which refers to carrying out the treatment for legitimate, specific, explicit, and informed purposes to the user and compatibility of the treatment with informed purposes. In LGPD the principle of "Necessity" – which refers to the limitation of treatment to the minimum necessary for the achievement of its purposes – is similar to GDPR principle of "Storage limitation". For LGPD principle of "Transparency" and "Accountability" in GDPR we have "Lawfulness, fairness and transparency" and "Accountability" as well. In GDPR "Integrity and confidentiality" is the same purpose described for LGPD principle of "Security". The principle of "Free Access" in LGPD speaks about a guarantee, to the holders of the data collected, of accuracy, clarity, relevance and updating of the data; similar to GDPR principle of "Accuracy". For LGPD we have the principle of "Data quality" which is similar to the concept of "Data minimisation" in GDPR. At last, but not least, LGPD has two more principles, they are: "Prevention" – adoption of measures to prevent the occurrence of damages due to the processing of personal data – and "Non-discrimination" – impossibility of carrying out the treatment

for illicit or abusive discriminatory purposes.

2.3.1 Consent of the Data Subject

In terms of the rights of data subjects, Article 4 of the GDPR defines a *consent* as any indication that is freely provided, specific, informed, and unequivocal of the data subject's wishes. By expressly affirming their consent, they indicate that they agree to the processing of his personal data [GDPR, 2019].

In the same sense, the LGPD presents a similar definition in its Article 5, paragraph XII, which says: "consent is a free, informed and unequivocal manifestation by which the holder agrees with the treatment of his data for a specific purpose" [Lei N° 13.709, 2018].

Thus, from the articles mentioned above, the following constitutive elements of valid consent are found: (a) free consent; (b) informed; (c) unambiguous; and (d) for a specific and determined purpose.

According to Chassang [2017], the concept of consent has been specified in terms of its specific characteristic, which eliminates any uncertainties regarding the scope of activities that the data subjects have consented to, as well as the type of consent that should be a declaration or explicit affirmative action.

2.4 Privacy by Design (PbD)

A pioneering concept developed by the Ontario Information and Privacy Commissioner has been called *Privacy by Design* (PbD). The concept was developed in the 1990s and has gained international recognition since then, being covered by GDPR and LGPD, it is a great ally in adapting to legislation, as it is a good practice in personal data processing operations. Cavoukian [2009] stresses that the future of privacy cannot be governed solely by regulations; rather, privacy protection should be a standard operating model for organizations.

Rather than being reactive, privacy by design is a proactive approach that accounts for privacy implications of new technologies at the time of development, not as an afterthought. There are seven principles for PbD:

1. **Proactive not reactive:** by preventing privacy risks from occurring, PbD does not offer remedies to resolve privacy violations once they occur, nor does it try to resolve them once they have occurred. This principle can be associated with LGPD principle of "Prevention".
2. **Privacy as the default setting:** in the context of PbD, the goal is to safeguard personal data in all IT systems and business practices automatically. In the absence of individual actions, personal data remains secure. This principle can be associated with LGPD principles of "Purpose", "Adequacy" and "Necessity". Similarly, for GDPR it is associated with the principles of "Purpose limitation", "Data minimisation" and "Storage limitation".
3. **Privacy built into design:** this is not an afterthought. Consequently, privacy becomes a core component of the functionality that is being delivered. The system provides privacy without compromising functionality.

4. **Total functionality - positive sum, not zero:** despite false dichotomies such as privacy versus security, PbD shows it is possible and preferable to have both.
5. **End-to-end security - ensuring complete lifecycle protection:** the information will remain secure during the entire process, and will be destroyed in a timely manner after it has concluded. LGPD and GDPR laws, respectively, recognize this principle with “Security” and “Integrity and confidentiality”.
6. **Commitment to visibility and transparency:** for both users and providers, its components and operations remain visible and transparent. It is the responsibility of each organization to document and communicate its privacy policies and procedures. LGPD acknowledge this principle with the principles of “Transparency” and “Accountability”. Likewise, GDPR connect this principle with “Lawfulness, fairness and transparency” and “Accountability”.
7. **Respect for user privacy:** provides strong privacy defaults, appropriate notice, and user-friendly options while keeping the interests of the individual at the forefront. This principle can be associated with LGPD principles of “Free access” and “Data quality”; and for GDPR with the principle of “Accuracy”.

The principles of “Privacy built into design” and “Total functionality - positive sum, not zero” has no direct link with the principles listed in GDPR and LGPD laws. However, they are principles that help to deal with privacy concerns.

Figure 1 summarizes the relationship between the principles of PbD and the principles described in the laws LGPD and GDPR.

2.5 Related Work

The study summarized in Wu *et al.* [2018] highlights a heuristic model that detects users’ behavioral inconsistencies in three aspects: request type and sensitivity, others’ disclosure willingness, and the experience of collaboration (*crowdsourcing*). The authors evaluate six hypotheses, with which they verify whether the disclosure behavior of users is expressed in volume and variability. They also identify differences between younger and older users, as well as between professionals and non-professionals, that may produce inconsistencies and errors within the model. The authors requested items in two categories: context (requests that are mainly related to a person’s online experience) and demographic.

An initial pilot study was conducted to determine whether the proposed heuristics might cause inconsistent sharing behaviors among participants. For the main study, there were 774 participants assembled up of Chinese citizens aged 18 to 65.

Moreover, the authors demonstrate that some users may be persuaded to alter their disclosure behaviors in a manner that is more consistent with the preferences of the system. In this way, the following hypotheses were supported: (a) requesting sensitive items first reduces subsequent disclosures by users, and (b) asked items answered by experienced participants show minor variation in the volume of exposure than requested items answered by less experienced partici-

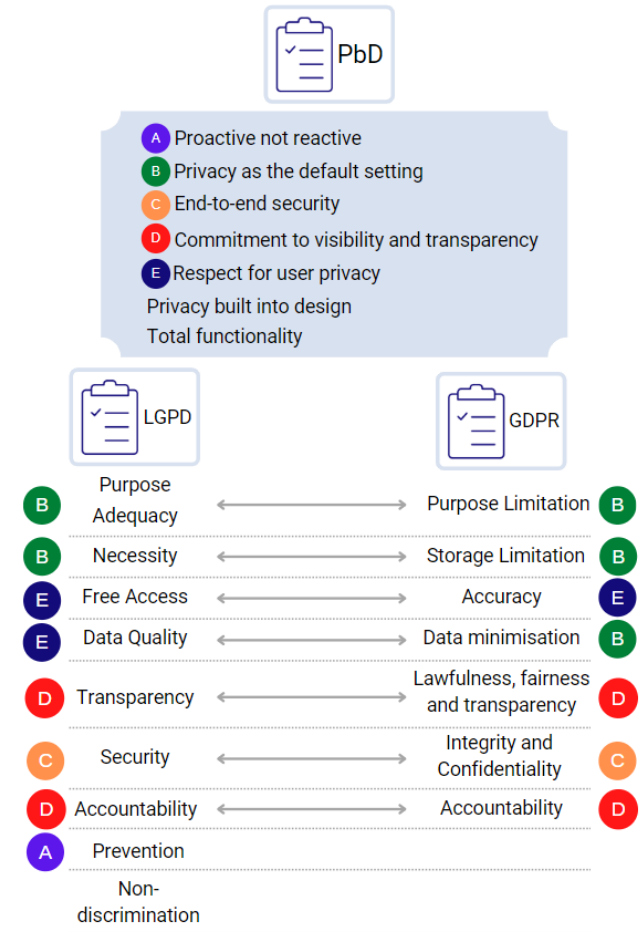


Figure 1. Relationship between the principles of Privacy by Design (PbD), General Data Protection Law (LGPD), and General Data Protection Regulation (GDPR)

pants. The following hypotheses were partially supported: (a) the request type influences the prediction of participants’ next disclosures, and (b) requesting sensitive items affects the prediction accuracy of the users’ next disclosures. The following hypotheses were not supported: (a) requesting demographic items first will not increase the users’ subsequent disclosures versus requesting context items first, and (b) the Spearman’s Rho values between two closely related items and between two remote items among experienced participants is not less variable than among less-experienced participants.

The work of Albeshier and Alhussain [2021] evaluate and compare the usability of privacy in WhatsApp, Twitter, and Snapchat. In this evaluation, the structured analysis of privacy (STRAP) framework was used. The STRAP heuristic is a framework with a focus on user design. It acts as a privacy awareness tool when applied to design projects.

A team of seven expert evaluators applied the 11 STRAP heuristics to the privacy policies and settings provided by WhatsApp, Twitter, and Snapchat. By providing understanding of the term “usable privacy”, this paper will help improve the usability of privacy settings and policies in social media.

The STRAP heuristics studied are Notice/Awareness (available, accessible and clear; correct complete, and consistent; presented in context; not overburdening), Choice/Consent (meaningful options; appropriate defaults;

explicit consent), Integrity/Security (awareness of security mechanisms; transparency of transactions), and Enforcement Redress (access to own records, ability to revoke consent).

Snapchat consistently had the highest rating for each heuristic, except for meaningful options and access to a user's own records, where WhatsApp had the highest ratings. Except for three heuristics, Twitter had higher usability problem ratings than WhatsApp.

3 Methodology

The inspection methodology applied in this study was the heuristic evaluation, focusing on privacy heuristics that influence Facebook users to disclose information and define what data they give consent, and by whom it can be seen. This analytical method aims to identify problems according to a set of heuristics or guidelines. The process involved four steps, the initial phase involved steps 1 and 2 and the evaluation phase involved steps 3 and 4. They are: 1) Select a set of privacy heuristics to inspect; 2) Identify the most popular features on Facebook which are used by users; 3) Inspect the Facebook's interface to identify heuristics that influence users data disclosure; 4) Review observations and results gathered during the inspection.

Figure 2 shows those activities and the following paragraphs describe them in more detail.

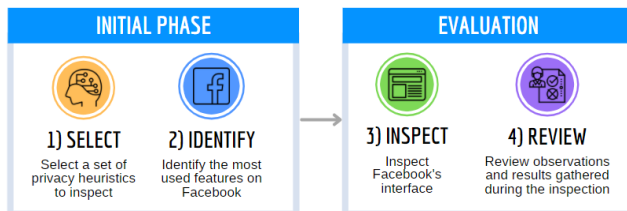


Figure 2. Inspection methodology proposed for the evaluation of Facebook regarding users privacy concerns.

During the step (1) *Select a set of privacy heuristics to inspect*, a literature review was carried out to survey cognitive heuristics that influence individuals' decisions to protect or renounce privacy. As such, this research had an exploratory nature. As for the technical procedures used, a bibliographic survey was carried out on the subject in question. In this survey, we examined several of the computing world's digital repositories, including the Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), Springer, and Science Direct. By using the terms (privacy AND heuristic) and (heuristic AND disclosure), articles were searched by title and subject.

After this survey, a total of 25 articles were returned from the digital repositories, which has been read in full for the selection of privacy heuristics. The authors cited identified heuristics that influence the dissemination of information from users, which is the focal point of this study. Other studies, not mentioned, did not present heuristics with the characteristics discussed above, in which investigations observed that addressed aspects related to the usability (Nielsen's

heuristics) and security; other works presented heuristic algorithms to preserve privacy. Thus, a set of heuristics identified in the results of the research studies prepared by the authors were compiled at the end, Gambino *et al.* [2016], Vincent *et al.* [2017], and Sundar *et al.* [2020]. The results of this survey are presented in Section 4.1.

For the step (2) *Identify the most used features on Facebook by users*, it was evaluated through research on news sites what the company's president, Mark Zuckerberg, points out as a trend among users worldwide. According to Zuckerberg, users' movement is towards disseminating videos and the language of stories, publications that are available for a maximum period of 24 hours. In 2018, Mark Zuckerberg reported changes in the company's strategies, bringing three major trends and challenges [Agência Brasil, 2018]. These being:

1. Change of people from traditional social networks to private messages and the language of stories;
2. Growth of video between the platforms, which is forecasted that in the next ten years the forms of interaction will be based on groups, or "communities";
3. Concerns related to users' "security threats".

In 2021, 15% of all Facebook content was video, in which 85% of Facebook videos were watched with no sound. Over 1.8 billion (62% of MAUs) Facebook users have joined Groups, and 500 million people use Facebook Stories daily. Facebook is used by more than half of the people actively to search for products, and most of them discover new products through the News Feed, Pages, and Groups on Facebook; also 800 million monthly active users are on the Marketplace [Social Media Perth, 2021; Omnicore, 2021; Oberlo, 2021].

Zuckerberg changed the name of the company to Meta in October 2021. He stated that the company's focus is on bringing the metaverse to life and enabling people and businesses to connect, find communities, and grow their businesses through augmented and virtual reality. They envision that people can benefit not just as consumers but as creators. Also, they promised that privacy and safety are going to be added from day one (PbD) [Meta, 2021].

In step (3) *Inspect Facebook's interface*, we sought to identify whether Facebook implements the selected heuristics, identified in step 1, in its functionalities available to the social network users. The Facebook platform was inspected - trying to complete tasks and going through the different moments of the experience, which, as mentioned in step 2, were considered a tendency of the social network users. The evaluated points of the social network platform were verified in the web and mobile versions.

The heuristic evaluation counted with the participation of three expert evaluators, two of them have experience in Characterizing and Modeling Online Social Network User Behavior, including Privacy and Information Security issues, and one in the area of Human-Computer Interaction, especially in the areas of Usability and Accessibility.

Heuristic evaluation involves having a small set of evaluators individually examine the interface and judge its compliance with recognized usability principles (the usability "heuristic"). In this work, instead of evaluating usability using usability heuristics, we evaluate Facebook based on the

privacy heuristics raised in step 1, which favor the increase or inhibition of information disclosure.

Furthermore, the evaluators discussed and decided together which Facebook features would be evaluated and which heuristics to use. We investigated the publication functionality regarding Zuckerberg's first challenge, considering the publication of stories directly on the timeline or in groups. Given the selected heuristics, we analyzed the section of Marketplace of the social network. For the second challenge, we inspected the form of interaction available between individuals in groups, government agencies, public figures, media companies, or brands. For the third challenge, we evaluated the available "Settings and privacy" options.

After the inspection of the interface, carried out individually by each specialist, it was conducted the step (4) *Review observations and results gathered during the inspection*. After cross-examination of the problems and aspects identified by each specialist, we maintained the consensus observed among the evaluators.

In Section 4.2, the observations and results obtained during the inspection of the social network are reported. This paper presents a comparison of the cognitive privacy heuristics identified in the literature. We bring a critical point to evidence the activation of such heuristics when performing a specific interface task. Such analysis format is applied in terms of consent to data disclosure. Contrasts are presented with the concepts of Privacy by Design (Section 2.4) and the regulatory principles present in the GDPR and LGPD laws (Section 2.3).

4 Results and Discussions

This section presents the results obtained with the survey of privacy heuristics found in the literature and the result of the evaluation carried out on Facebook based on these heuristics.

This work contributes to the privacy area in the sense of bringing these heuristics, which can be applied to any other social network, in addition to the analysis of how much Facebook complies with these recommendations.

4.1 Privacy Heuristics

This subsection presents papers that identified privacy heuristics that influence individuals' personal data disclosure decisions which increase or inhibit information disclosure.

4.1.1 Heuristics of Gambino *et al.*

In the study conducted by Gambino *et al.* [2016], the authors conducted eight focus group sessions with 41 participants. Three groups were formed by university students and five by individuals who were not students. A semi-structured set of questions was administered to each group throughout the study to assess the individuals' behavior related to privacy, from broad perceptions and behaviors to specific actions. In general, the questions covered six main topics of interest: privacy and security, mobile, e-commerce, messaging, cloud computing, and social media.

The authors of these experiments identified four heuristics referred to as *positive* that were found to be effective in facilitating users' engagement in online or mobile contexts. They are: (1) *Gatekeeping*: the users prefer a system that adopts clear measures to protect their information, such as using two-factor authentication¹ (2) *Safety Net*: users have as their premise the confidence that third-party services, such as Visa, PayPal, and Apple, will guarantee the security of their personal information. (3) *Bubble*: Users reported a greater sense of security when using anonymous browsing modes or when conducting transactions on the home network. (4) *Ephemerality*: On platforms like *Snapchat*, participants are more comfortable exchanging information. According to the authors, when the heuristic is activated, users feel more comfortable and open to sharing more information, as there is no permanent record or record which can be accessed by others.

Four additional heuristics were identified as *negative*, in which individuals distrust a site or restrict the sharing of information. (1) *Fuzzy-boundary*: users expressed discomfort when faced with constant evidence of their browsing behavior online. An example of this is advertisements directed at the individual, causing the suspicion that the information is shared with third parties without their knowledge or consent. (2) *Intrusion*: associated with the inconvenience of receiving unsolicited e-mails or notifications and announcements, which leads the user to question the integrity of the system that makes or allows the request. (3) *Uncertainty*: concerning the feeling of discomfort caused by an unknown situation in which an individual feels insecure due to an inability to comprehend the device or website. One example of this is users' skepticism about cloud services. (4) *Mobility*: these are concerns inherent in the use of mobile products, which may be associated with concerns about the Internet used or the theft of devices.

4.1.2 Heuristics of Vincent *et al.*

In the study conducted by Vincent *et al.* [2017], 23 semi-structured individual interviews were conducted with users between 18 and 25 years old. The authors identified six classes of heuristics that users trust during disclosures, they are: *Prominence*, *Network*, *Reliability*, *Agreement*, *Modality* and *Narrative*.

The class **Prominence** allowed us to observe that, in general, if something gained Prominence, it must be doing something right, while the lack of it suggests the opposite. Therefore, this class comprises two heuristics, namely: 1) *Reputation*: for which it is considered that a prestigious service would not consciously do something wrong, referring to judgments of credibility concerning the legitimacy of an organization. 2) *Recognition*: in which the main difference is that such Reputation extends beyond the original entity towards the subsidiaries, similarly defined by Gambino *et al.* [2016] as "Safety Net".

The class **Network** is observed through the perception of the influence that an individual's interpersonal network has on disclosure decisions. It is evidenced through heuristics,

¹Added a second layer of verification triggered to confirm the user's identity when performing login on some service online.

such as 1) *Endorsement*: recommendations from acquaintances are preferred over self-recommendations; 2) *Bandwagon*: extends to recommendations from strangers received for less personal factors, such as aggregated testimonials or star ratings embedded in the interface. 3) *Authority*: when trust derives from recommendations by official authorities or experts. According to Vincent *et al.* [2017], herd behavior can arise without due consideration of circumstances, with the expectation that others will discover the risks inherent in an information disclosure decision.

The class **Reliability** contains three heuristics: 1) *Consistency*: based on trust about the agreement between independent sources, being observed when it becomes evident that a non-standard requirement for registration is a consistent service requirement similar; 2) *Consensus*: this is a standardized and general agreement, for example, to interact on a social network, it is expected that the name, email and profile picture will be informed; and 3) *Expectation*: for which negative connotations may arise around the deficient interface design, in which there is an expectation of professionalism. According to Vincent *et al.* [2017], the three heuristics are linked to the idea that if something is broken, has errors, or something changes, this can lead users not to disclose information.

The class **Accordance** differs from the class *Reliability*, as it refers to beliefs and understanding rather than processor interface. In this class, two heuristics are present: 1) *Self-confirmation*: triggered when something aligns with a previous belief, not requiring a norm for requesting information, as long as there is an understanding that the request “appears for good reasons”. 2) *Persuasive Intent*: whose underlying principle is that perceived manipulation leads to negative judgments. Gambino *et al.* [2016] call this “*Intrusion*”, as the case where the user tries to interact with a site and pop-ups appears, for example. Furthermore, according to Vincent *et al.* [2017], with the removal of the word “*Persuasive*”, the heuristic (“*Intent*”) would serve a purpose close to the element of integrity in Gambino *et al.* [2016].

The class **Modality** includes heuristics: 1) *Coolness*: associated with new technological resources, or the bells and whistles of existing technologies, with positive assessments of credibility; and 2) *Novelty*: subtly different from the heuristic *Coolness*, being invoked by a user’s initial experience with technology.

According to the study, the class **Narrative** is symbolized by the absence of narrative, i.e., consideration of the risks involved with excessive disclosure [Norberg *et al.*, 2007]. When faced with a particular decision, individuals may choose to disclose more information when influenced by this class. There are two heuristics: 1) *Availability*: refers to a judgment of the probability of an event based on the “ease with which relevant instances come to mind”. 2) *Coherence*: related to the ability to view the outcome of a decision as a plausible consequence. According to Vincent *et al.* [2017], it is not satisfactory to wait for users’ negative experiences to instill a more cautious and considered approach to disclosure. Instead, it may be possible to inform users about the risk of disclosure through a relatable narrative.

A seventh class **Trade**, non-heuristic², was also recognized that respondents were also evaluating their disclosures in terms of commercial utility gains versus losses. According to the authors, although users demonstrate efforts to disseminate information more inductively, after considering a sufficient number of particular cases, the variables underlying the decision made generally remain based on heuristics.

4.1.3 Heuristics of Sundar *et al.*

In the study conducted by Sundar *et al.* [2020] twelve heuristics derived from the privacy literature online were selected and are organized in terms of three privacy contexts: 1) *social*, refers to contexts that presuppose the existence of the influence of other individuals concerning the user decisions; 2) *personal*, referring to situations that focus on the individual as an autonomous entity, in which users seek to maintain their privacy or disclose information to protect, extend or improve themselves; and 3) *technological or environmental*, refers to elements of the physical space.

In the **social** context, six heuristics associated with higher dissemination intentions are identified, they are: (1) *Authority*: the presence of a well-known name, brand or organization on a website is likely to cause users feel safe, taking the mental shortcut that everything they do and reveal on the site is secure; (2) *Bandwagon*: if the majority of users in a online community show information for a website, then the tendency is for the user to also opt for disclosure; (3) *Reciprocity*: a common rule of interpersonal communication whereby intimate self-disclosure follows the principle of reciprocity - if the partner reveals something personal, the tendency is to reciprocate, revealing something equally personal about himself; (4) *Sense of Community*: when people feel part of a community, they can trust and depend on each other for support, and ultimately share more intimate aspects of their lives with each other; (5) *Community Building*: a robust online forum is the result of active participation by users. The sharing of personal information can contribute to community building in this manner; (6) *Self-presentation*: the purpose of revealing personal information online is to enhance social status in online social settings.

In the **personal** context, two heuristics associated with higher disclosure intentions are identified, they are (1) *Control*: providing users with the ability to control the pace and nature of content is a way to trigger the control heuristic, resulting in a favorable perception of the interface and its content; (2) *Instant gratification*: individuals are driven by an “optimism bias”, which makes them respond promptly to instant offers online and underestimate the risks of disclosing information in the process.

Four heuristics related to disclosure have been identified within the **technological** context. There are two heuristics related to *positive* disclosure intentions. (1) *Transparency*: in explaining what it is and how user information is used, the privacy policy statements and the explicit demonstration of permissions can impose credibility on a web site, which the user has a tendency to trust due to the full disclosure of its

²Decision making that fights any confirmation bias; predicting the risk involved and acting with caution.

policies; (2) *Machine*: there is a belief that machines would manipulate information according to legal rules and have no human weaknesses such as gossip; the author discusses interactions with voice assistants such as Siri, Cortana and Alexa. Additionally, two additional heuristics are associated with *negative* disclosure intentions. (1) *Publicness*: users express deeper privacy concerns when they are on a wireless network, with a feeling of vulnerability when carrying out transactions using public networks; (2) *Mobility*: users, whenever reminded that they are on a mobile device, tend to trigger the mobility heuristic; therefore avoiding storing private information.

In Figure 3, privacy heuristics that increase information disclosure behavior are illustrated. Contrary to this, Figure 4 reveals privacy heuristics that inhibit information disclosure. Figures 3 and 4 synthesize privacy heuristics pinpointed by Gambino *et al.* [2016]; Vincent *et al.* [2017]; Sundar *et al.* [2020].

4.1.4 General Considerations About the Heuristics Presented

The conclusions reached by the authors cited Gambino *et al.* [2016]; Vincent *et al.* [2017]; Sundar *et al.* [2020] corroborate the relevance that cognitive privacy heuristics play in supporting users' decision-making regarding clear and precise information about the online services used.

Wu *et al.* [2018] concludes that users provide more information for moderated items when they have no prior knowledge. In comparison, the heuristic model may persuade others who do not have prior knowledge to support their decision-making to disclose more information. This issue was also observed in the work of Gambino *et al.* [2016], who found that individuals generally act with little thought or evaluation, even showing surprise when faced with their behaviors.

In the same sense, Vincent *et al.* [2017] states that users tend to make poor decisions and that regulatory efforts that seek to increase the autonomy of the informed user are inept. The authors reinforce that cognitive heuristics are essential to understand users who consent to disclose more than intended (i.e., privacy paradox). Nevertheless, to understand users who agree to reveal more than they know (i.e., simple consent). Therefore, the authors suggest that the key to supporting users during disclosure decisions may be to push users through tips that favor the triggering of cognitive privacy heuristics positively.

Sundar *et al.* [2020] confirm their hypothesis that users' belief (or degree of accessibility) in a given heuristic is significantly associated with their intentions to reveal private information in a disclosure context that presents a suggestion outlined to trigger a given heuristic. Also, the authors noted the significant role that interface tips played in influencing a user's decision to share private information.

Regarding the authors' considerations previously mentioned, Ghaiomy Anaraky *et al.* [2021] identified that younger adults rely more heavily on heuristic decision-making, being more likely to change their perception of data sensitivity based on trust. Conversely, older adults were

more likely to disclose information that they perceive to be of value, whereas they were less likely to disclose information that was influenced by heuristics.

4.2 Inspection of Privacy Heuristics on Facebook

This section presents the result of the heuristic evaluation carried out on Facebook based on the heuristics raised that favor the increase or inhibition of information disclosure.

For the inspection of Facebook, the functionalities described in step 2 of Methodology, page 6, were considered:

1. Change of people from traditional social networks to private messages and the language of stories;
2. Growth of video between the platforms, which is forecasted that in the next ten years the forms of interaction will be based on groups, or "communities";
3. Concerns related to users' "security threats".

4.2.1 Heuristics that Increase Information Disclosure Behavior (Positive)

The following items expose factors observed during the inspection of Facebook that can proportionate a positive influence for users to continue interacting and sharing content.

- **Gatekeeping**: it is possible to enable two-factor authentication for cases where the user uses Facebook as a form of authentication in other applications. Additionally, the possibility of configuring a one-time password is provided for applications that do not support two-factor authentication (example: Xbox, Spotify). The presence of Gatekeeping on Facebook favors a more secure control of access to the user's account. It is an example of PbD principles "End-to-end security - ensuring complete lifecycle protection" and "Proactive not reactive". For LGPD principle it speaks about "Security" and for GDPR the principle of "Integrity and confidentiality".
- **Safety Net**: in the Marketplace area of the social network, it is possible to advertise products for sale/rent, and you can view ads from anyone on the network. However, Facebook does not allow adding a payment method. In this case, space works only as propaganda, and it is up to users to negotiate the purchase and sale of published products. Using the tool, users are able to search for advertisements based on their current location on their phones.
- **Ephemerality**: one of the available forms of publication is through stories where the user makes a post. According to his defined configuration, it will be available for 24 hours for the "Public", "Friends", "Custom" or "Hide story from". Since Facebook allows user to control to who the post is available it makes possible for users' to consent to disclose information without sharing it with everyone in the social network. It is an example of PbD principles "Respect for user privacy" and "Privacy as the default setting". For LGPD it speaks



POSITIVE

Heuristics that increase information disclosure behavior

Gatekeeping¹

Adopts clear measures to protect users' information

Safety Net¹

Implements third-party services

Ephemerality¹

Makes information last for a brief time

Bubble¹

Brings a sense of security when using anonymous browsing or conducting transactions at home network

CLASSES OF HEURISTICS

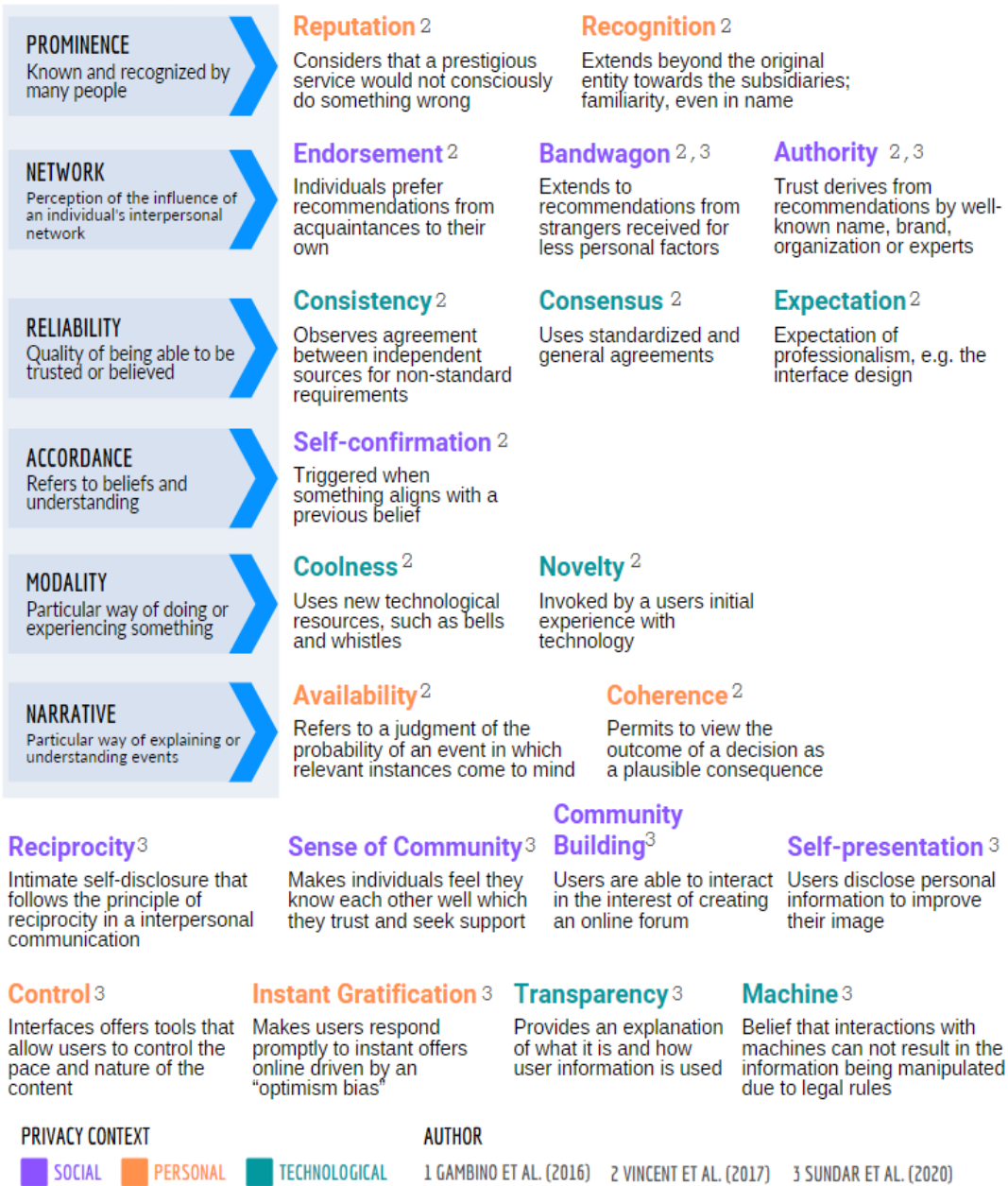


Figure 3. Positive privacy heuristics that increase users information disclosure.

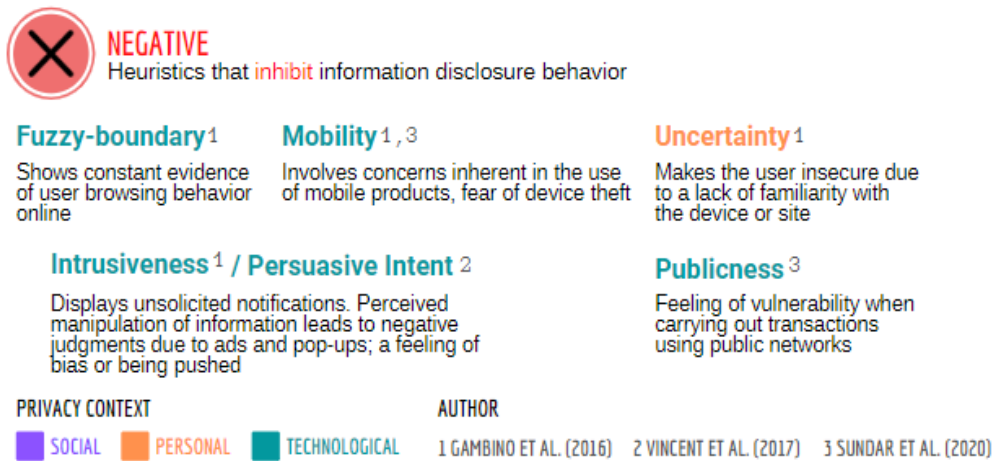


Figure 4. Negative privacy heuristics that inhibit users information disclosure.

about the principle of “Necessity” and for GDPR the principle of “Storage limitation”.

- **Prominence (Reputation and Recognition):** even though Facebook was involved in the Cambridge Analytica scandal in 2018 – a political consultancy that misused user data to affect elections in the United States – the company has demonstrated a commitment to managing social issues. In 2021, the social network completed 17 years of existence, totaling 2.9 billion monthly active users and dominating the social media market for a decade [Statista, 2021; Ortiz-Ospina, 2019]. Facebook Reputation and Recognition allows it to continue having users opting to use the platform to communicate with other individuals.
- **Reliability (Consistency, Consensus and Expectancy):** The Engineering at Meta [2017] page exposes the continuous delivery scale approach adopted by the platform, which divides the process into three layers: development, static analysis and testing. The constant delivery cycle enables the user experience to be better and faster. According to Meta [2018] page the team has been working to review and expand their tools to help people manage privacy and understand their choices regarding personal data. The class Reliability is an example of PbD principle “Privacy built into design”. The heuristic Consensus also applies the PbD principles of “Respect for user privacy” and “Privacy as the default setting”. Regarding the GDPR Consensus apply the principle of “Data minimisation” and for LGPD the principle of “Data Quality”.
- **Modality (Coolness and Novelty):** the social network shows focus on the customer, providing improvements based on the interests of its users. A good example of this is the personalized reactions to publications. In 2020, for example, Facebook launched the reaction “Care”, Figure 5 (a) whose aim was to help social network users express support to each other during the pandemic of coronavirus (COVID-19). Another example is when someone receives a “congratulations” and can click/tap on the word. The interface can display an animation of confetti, balloons, and stars. See Figure 5 (b).

This is an example of cosmetic changes made into the platform that creates a desire to use those features while posting.

- **Narrative (Availability and Coherence):** When using the Facebook interface, it is possible to perceive **availability** and **coherence** in the available features. For example, when performing an action and not saving, the user is asked to confirm whether he/she wants to leave without ending, Figure 5 (c).
- **Network (Endorsement, Bandwagon, Authority):** Facebook provides interaction between individuals, where they request and provide recommendations to acquaintances or not, thus being able to trigger the endorsement heuristics and Bandwagon, respectively. Regarding the Authority heuristic, there is a “seal of authenticity” on the social network, intended for well-known and well-researched pages and profiles, which validates as authentic posts made by government agencies, public figures, media companies, or brands.
- **Sense and Community Building:** as previously mentioned in Section 3, it is projected that in the next ten years, the forms of interaction will be based on groups. With this in mind, Facebook presents a section on the main menu bar to keep track of the user’s recent “Groups” activities.
- **Instant gratification:** heuristic not identified during the social network inspection.
- **Control:** in both browser and mobile application access, the interface encourages and gives the user tips on steps they can take to manage the data they want to share and which individuals they want it to be visible. At the level of *individual* privacy, Facebook allows the user the four fundamental states of interaction with other people (loneliness, intimacy, anonymity, and reservation). When choosing the audience with which the user wants to share certain information, for example, phone number, email, date of birth, and publications, it is possible to set to “Public”, “Only me”, “Friends”, “Friends except acquaintances”, “Custom”, among others. Same as Ephemerality, Facebook allows user to control to who the post is available, by doing so, the user

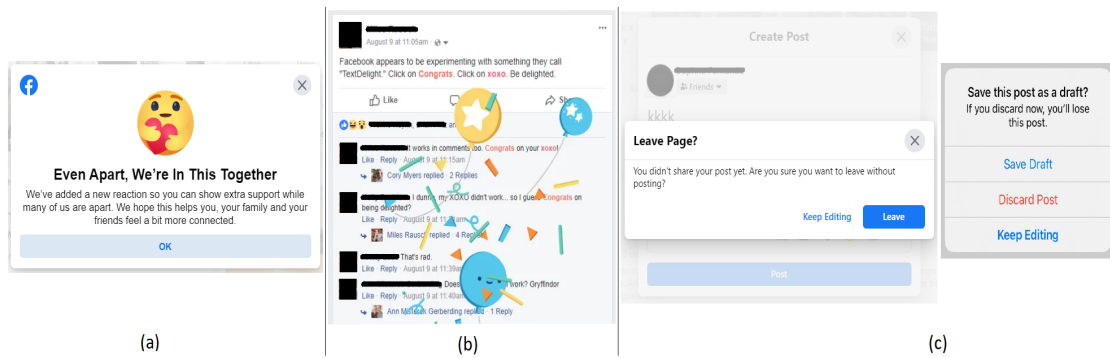


Figure 5. (a) “Care” reaction added by Facebook in indication of awareness with the social distance imposed by the COVID-19 pandemic; (b) Effect of the word “congrats” written in a post when clicked/touched; (c) Confirmation that you want to leave without finishing the action previously started.

Source: <https://facebook.com/>

gives consent to disclose information without sharing it with everyone in the social network. Also, Meta [2018] shows that Facebook made a commitment to simplify the design of their privacy settings in a new control center and to notify users in their feed to verify their privacy configuration, features observed during the evaluation. It is an example of PbD principle “Respect for user privacy” and “Privacy as the default setting”. For LGPD principle it speaks about “Security” and for GDPR the principle of “Integrity and confidentiality”.

- **Transparency:** because of regulatory measures such as GDPR and LGPD, Facebook allows users to establish rules regarding the collection, storage, treatment, and sharing of their data. The settings and privacy tools’ area allows the user to view the information accessible (Figure 6 a). It is an example of PbD principle “Commitment to visibility and transparency” and also “Privacy as the default setting”. In regards to LGPD it speaks about the principle of “Transparency” and for GDPR the principle of “Lawfulness, fairness and transparency”.

More specifically, according to Oliveira *et al.* [2021], when the user experience is positive enough it can influence users to continue using the technology. Furthermore, the level of complexity of a system should be proportional to the expectations of the target audience. As an alternative to the heuristics observed, cultural factors may affect the perception of relative advantages, such as ethical, privacy, or gender issues. The factors listed above also contribute to the user experience and the decision to disclose personal information.

4.2.2 Heuristics that Inhibit Information Disclosure Behavior (Negative)

During the inspection of a post-publication, we inspected the navigation in Facebook’s timeline. The activation of the **intrusiveness/persuasive intent** heuristics happened due to the appearance of sponsored advertisements among the posts of connections and groups. Such occurrence, at first, can cause the user some discomfort, leading him to be also influenced by the heuristics of **uncertainty** and **fuzzy-boundary**. By default, the social network’s ad configuration is set to “Al-

lowed”, which is contrary to the PbD principle of “Privacy as the default setting”, and this setting should be initially set to “Not Allowed”.

It should be noted that for those users who are looking for a higher level of interactivity with the interface, Facebook offers in the post word “Sponsored” a URL that directs the user to a page. On the page, users are invited to understand better how the publicity work and how user data is used to show ads Facebook [2020]. In the same way, in the “Privacy shortcuts” area, it is possible to check the ad preferences (Figure 6 b).

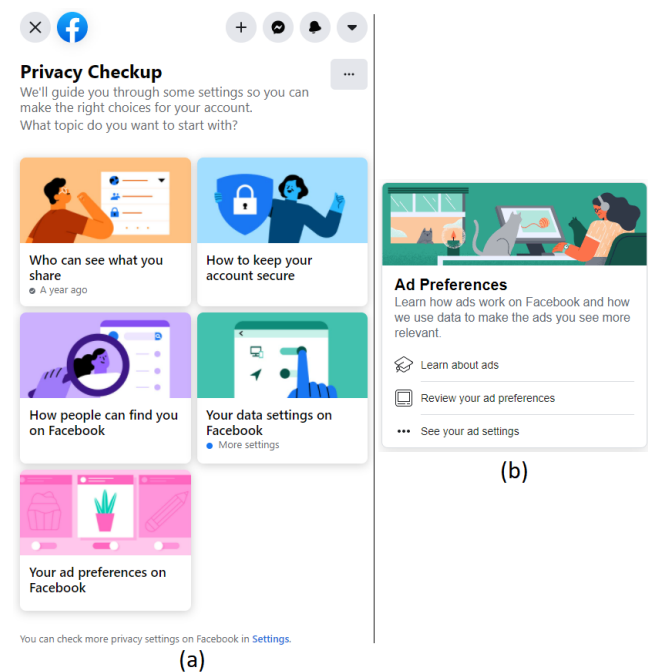


Figure 6. (a) Privacy Checkup Page created to guide users through how to manage data settings and (b) Ad Preferences guiding users on how ads are selected based on their data.

Source: <https://m.facebook.com/>

4.2.3 Heuristics not Evaluated in the Inspection Context

The “Bubble” heuristic was not evaluated during the inspection because its activation was associated with anonymous browsing mode or home network. The heuristics “Self-confirmation”, “Reciprocity” and “Self-presentation” were also not evaluated because they are associated with the user’s beliefs, interpersonal communication, and willingness to self-disseminate its image, respectively. The “Machine” heuristic was not evaluated because it refers to the idea that machines would manipulate information according to legal rules. Finally, the heuristics of “Mobility” and “Publicness” were also not evaluated since the characteristics that inhibit users’ disclosure behavior are directly related to vulnerability when connected on public Internet networks or while using mobile devices (prone to theft).

Thus, Table 1 presents the grouped result of the cognitive privacy heuristics that were (or were not) observed during the inspection on Facebook.

Table 1. Results of privacy heuristics observed during heuristic evaluation on Facebook.

Class ²	Heuristic		
Positive	<i>Gatekeeping</i> ¹	✓	
	Safety Net ¹	✗	
	Bubble ¹	N/A	
	Ephemerality ¹	✓	
	Prominence	Reputation ²	✓
		Recognition ²	✓
	Reliability	Consistency ²	✓
		Consensus ²	✓
		Expectancy ²	✓
	Accordance	Self-confirmation ²	N/A
	Modality	<i>Coolness</i> ²	✓
		Novelty ²	✓
	Narrative	Availability ²	✓
		Coherence ²	✓
	Network	Endorsement ²	✓
		<i>Bandwagon</i> ^{2 3 a}	✓
		Authority ^{2 3 a}	✓
		Reciprocity ^{3 a}	N/A
		Sense of Community ^{3 a}	✓
	Community Building ^{3 a}	✓	
Self-presentation ^{3 a}	N/A		
Instant Gratification ^{3 b}	✗		
Control ^{3 b}	✓		
Transparency ^{3 c}	✓		
Machine ^{3 c}	N/A		
Negative	Accordance	Intrusiveness ¹	✓
		Persuasive Intent ²	✓
	<i>Fuzzy-boundary</i> ¹	✓	
	Uncertainty ¹	✓	
	Mobility ^{1 3 c}	N/A	
<i>Publicness</i> ^{3 c}	N/A		

¹ Gambino *et al.* [2016] ² Vincent *et al.* [2017] ³ Sundar *et al.* [2020]

^a Social context ^b Personal context ^c Technological context
 Subtitle: ✓ - observed heuristic; ✗ - unobserved heuristic;
 N/A - heuristic not evaluated in the interface inspection.

4.2.4 Heuristics Relationship to Privacy by Design, LGPD and GDPR Laws

According to the results of the analysis, Facebook shows that they are concerned to comply with GDPR and LGPD laws. The platform offers the user mechanisms to manage their privacy settings. However, the user must decide how he/she would like to protect their privacy and at which level considering the four states of personal privacy (loneliness, intimacy, anonymity, and reserve) [Westin, 2003].

While examining the heuristics surveyed in the literature, we observed the principles of Privacy by Design, which are an ally in the process of conforming to legislation. PbD figures as a good practice in personal data processing and as described in section 2.4, it cover principles presented in LGPD and GDPR laws. Furthermore, while evaluating the interface of Facebook we noticed that there are privacy heuristics related to the principles of PbD, LGPD, and GDPR.

As mentioned before in Subsections 4.2.1 and 4.2.2, the heuristic of “Gatekeeping” correlate with the PbD principles of “Proactive not reactive” and “End-to-end security”; also relates to “Security” from LGPD and “Integrity and confidentiality” from GDPR. For PbD principle of “Privacy as the default setting” we observed the heuristics “Ephemerality”, “Consensus”, “Control”, and “Transparency”. The principle of “Respect for user privacy” is observed in the heuristics “Ephemerality”, “Consensus”, and “Control” which provides a positive experience. Although, the negative heuristic “Intrusiveness/Persuasive intent” may be perceived as a lack of respect for user privacy. The PbD principle of “Privacy built into design” is detected in the heuristics “Consistency”, “Consensus”, and “Expectation”. For the heuristic “Consensus” we relate it to the principle of “Data minimisation” and “Data quality” from GDPR and LGPD, respectively. The PbD principle of “Commitment to visibility and transparency” is detected in the heuristic “Transparency”.

Figure 7 illustrates the relationship between the heuristics and the principles of PbD and the principles described in the laws LGPD and GDPR.

The presence or absence of heuristics related to principles proposed in Privacy by Design (PbD), the General Data Protection Law (LGPD), and the General Data Protection Regulation (GDPR) could have a significant impact on privacy concerns depending on the purpose of the principle related to the respective heuristic. When heuristics are not associated with any principles, their presence or absence may affect the decision of the user to disclose information. Additionally, how the user’s privacy settings are configured may affect the perceived privacy impact of the information disclosed.

According to Díaz Ferreyra *et al.* [2018], users of Social Network Sites (SNSs) are generally not informed much about the privacy risks of online interaction. Furthermore, users who consent to data collection and processing (i.e., those who accept the privacy policies) are usually not informed about such risks before they give their consent. The absence of information modulates the perceived severity of privacy risks, thereby benefiting the service providers. In order to develop preventative technologies, as well as to shape public policies that promote privacy awareness on social networks,

risk communication and management must be explored.

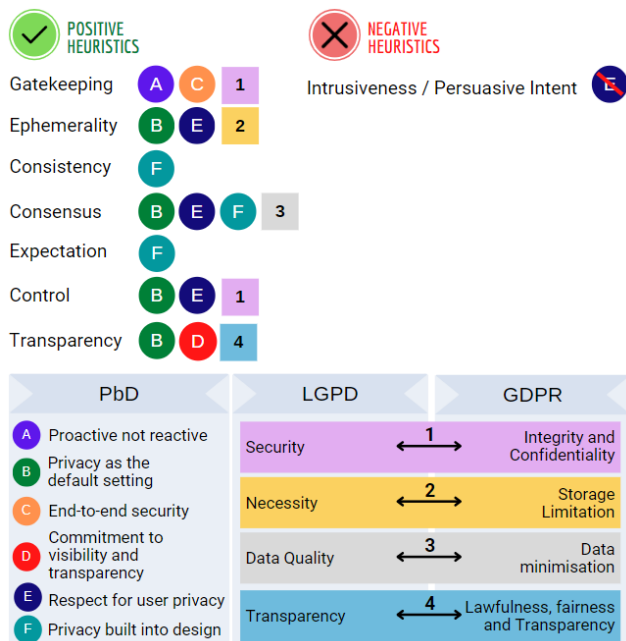


Figure 7. Relationship between the heuristics and the principles of Privacy by Design (PbD), General Data Protection Law (LGPD), and General Data Protection Regulation (GDPR)

5 Final Remarks

In the past decade, consumer privacy has become a priority issue for policymakers, given the numerous occurrences of personal information leaks that have made this a top candidate for legislation [Norberg *et al.*, 2007]. There is a concern with explicit consent among the subtopics addressed in legislative actions. Therefore, the user must provide his consent to the processing of his personal data by way of an affirmative statement or action.

Accordingly, this study investigated cognitive heuristics, which influence users when they only have a few seconds to decide whether to click on a URL or an option menu or checkboxes. The assessment of privacy by heuristic analysis showed that to make its system more secure and protect people’s privacy, Facebook has made available to its users measures on its privacy settings page, identifying the main characteristics of the protection of individuals’ data privacy [Michel Protti, Chief Privacy Officer, Product, 2020]. When analyzing the heuristics of “Transparency” and “Control” we noticed that Facebook allow users to control the collection, storage, treatment, and sharing of data in their privacy settings area.

By inspecting the heuristics “Ephemerality” and “Control”, it was possible to observe the PbD principle of “Respect for user privacy” and “Privacy as a default setting”. Another PbD principle recognized was the “Commitment to visibility and transparency” considering the heuristic “Transparency”. Furthermore, we noticed the PbD principle of “End-to-end security - ensuring complete lifecycle protection” and “Proactive not reactive” while observing the heuristic “Gatekeeping”. While examining the class of heuristics

“Reliability” we noticed the PbD principle of “Privacy built into design”. Therefore, the platform encourages the user to understand how their data is collected, stored, treated, and shared. As a result of such perceived aspects, a high level of information sharing between individuals is promoted and the GDPR and LGPD Laws compliance is shown because Facebook allows the user to manage their privacy settings accordingly.

On the other hand, during the investigation of heuristics that inhibit disseminating information, we noticed that the configuration of ads on the social network by default is defined as “Allowed”. While navigating the timeline can cause discomfort to the user because he feels confronted with the appearance of advertisements linked to his recent browsing interests. According to the PbD principle of “Privacy as the default setting”, such a setting should by default be set to “Not Allowed”.

In this way, identifying specific privacy-oriented heuristics can help the design community and software engineers design and evolve systems that present clues, suggestions, and opportunities for promoting safer and trustable computing. It is essential, however, that designers and software engineers use these heuristics ethically and avoid misleading users in order to reveal sensitive data that could compromise their privacy [Gambino *et al.*, 2016].

In this study, we noticed that interface tips play a critical role in triggering mental rules, dictating dissemination behaviors. Understanding the number and diversity of suggestions (heuristics) to which users are susceptible allows the creation of explicit guidelines to inform, alert and educate them, advancing knowledge in this area. Despite this, it appears that no set of operational heuristics has been developed that can operationalize the seven principles of PbD and the principles described in LGPD and GDPR laws.

From future perspectives, we aim to conduct a study with users of services online to formalize a set of privacy heuristics that operationalize the seven principles of Privacy by Design and the principles of LGPD and GDPR laws, enabling data controllers to demonstrate transparency about collecting, storage, treatment, and sharing individuals’ data.

Acknowledgements

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001. The authors thank the National Council for Scientific and Technological Development of Brazil (CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico) and the Foundation for Research Support of the Minas Gerais State (FAPEMIG). The work was developed at the Pontifical Catholic University of Minas Gerais, PUC Minas.

References

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221):509–514. DOI: 10.1126/science.aaa1465.

- Agência Brasil (2018). Facebook chega a 2,6 bilhões de usuários no mundo com suas plataformas. Available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2018-10/facebook-chega-26-bilhoes-de-usuarios-no-mundo-com-suas-plataformas>.
- Albeshar, A. S. and Alhussain, T. (2021). Evaluating and comparing the usability of privacy in whatsapp, twitter, and snapchat. *International Journal of Advanced Computer Science and Applications*, 12(8). DOI: 10.14569/IJACSA.2021.0120829.
- Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole Publishing Company. Book.
- Ataei, M., Degbelo, A., and Kray, C. (2018). Privacy theory in practice: designing a user interface for managing location privacy on mobile devices. *Journal of Location Based Services*, 12(3-4):141–178. DOI: 10.1080/17489725.2018.1511839.
- Baden, R., Bender, A., Spring, N., Bhattacharjee, B., and Starin, D. (2009). Persona: An online social network with user-defined privacy. In *Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication*, SIGCOMM '09, page 135–146, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/1592568.1592585.
- Cavoukian, A. (2009). The 7 foundational principles. Accessed 17 June 2019, Available at: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.
- Chassang, G. (2017). The impact of the eu general data protection regulation on scientific research. *Ecan-ecermedicalscience*, 11(709):1–13. DOI: 10.3332/ecan-ecer.2017.709.
- Díaz Ferreyra, N. E., Meis, R., and Heisel, M. (2018). At your own risk: Shaping privacy heuristics for online self-disclosure. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–10. DOI: 10.1109/PST.2018.8514186.
- Engineering at Meta (2017). Rapid release at massive scale. Accessed 17 June 2020. Available at: <https://engineering.fb.com/web/rapid-release-at-massive-scale/>.
- Estivill-Castro, V. and Nettleton, D. F. (2015). Privacy tips: Would it be ever possible to empower online social-network users to control the confidentiality of their data? In *Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015*, ASONAM '15, page 1449–1456, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/2808797.2809279.
- Facebook (2020). Sobre os anúncios do facebook. Accessed 24 June 2020. Available at: <https://www.facebook.com/ads/about/>.
- Gambino, A., Kim, J., Sundar, S. S., Ge, J., and Rosson, M. B. (2016). User disbelief in privacy paradox: Heuristics that determine disclosure. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '16, page 2837–2843, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/2851581.2892413.
- GDPR (2019). General Data Protection Regulation (GDPR). Accessed 20 October 2019. Available at: <https://gdpr-info.eu/>.
- Ghaiumy Anaraky, R., Byrne, K. A., Wisniewski, P. J., Page, X., and Knijnenburg, B. (2021). To disclose or not to disclose: Examining the privacy decision-making processes of older vs. younger adults. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, page 1–14, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3411764.3445204.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers Security*, 64:122–134. DOI: 10.1016/j.cose.2015.07.002.
- Lei N° 13.709 (2018). Lei n° 13.709, de 14 de agosto de 2018. Accessed 20 October 2019. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.
- Lei N° 14.010 (2020). Lei n° 14.010, de 10 de junho de 2020. Accessed 15 February 2021. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm.
- LGPD Brasil (2019). Lei Geral de Proteção de Dados (LGPD) – Lei n° 13.709/18. Accessed 20 October 2019. Available at: <https://www.lgpdbrasil.com.br/>.
- Meta (2018). Facebook apresenta novas opções para proteger dados e privacidade em conformidade com a gdpr. Accessed 23 June 2022. Available at: <https://pt-br.facebook.com/business/news/facebook-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr>.
- Meta (2021). Founder's letter, 2021. Accessed 19 December 2021. Available at: <https://about.fb.com/news/2021/10/founders-letter/>.
- Michel Protti, Chief Privacy Officer, Product (2020). Fighting platform abuse, simplifying privacy in groups, and protecting information while sharing data. Accessed 24 June 2020. Available at: <https://about.fb.com/news/2020/06/privacy-improvements/>.
- Neumann, G. K., Grace, P., Burns, D., and SurrIDGE, M. (2019). Pseudonymization risk analysis in distributed systems. 10:1–16. DOI: 10.1186/s13174-018-0098-z, journal = Journal of Internet Services and Applications.
- Nielsen, J. (1994). Usability inspection methods. In *Conference Companion on Human Factors in Computing Systems*, CHI '94, page 413–414, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/259963.260531.
- Norberg, P., Horne, D., and Horne, D. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41:100–126. DOI: 10.1111/j.1745-6606.2006.00070.x.
- Oberlo (2021). 10 facebook statistics every marketer should know in 2021. Accessed 12 December 2021. Available at: <https://www.oberlo.com/blog/facebook-statistics>.
- Oliveira, M., Mattedi, A., and Seabra, R. (2021). Usability evaluation model of an application with emphasis on

- collaborative security: an approach from social dimensions. *Journal of the Brazilian Computer Society*, 27:3:1–32. DOI: 10.1186/s13173-021-00108-8, url = , publisher = Springer Open, keywords = usability, innovation diffusion, access to technology, social factors.
- Omnicores (2021). 63 facebook statistics you need to know in 2021. Accessed 12 December 2021. Available at: <https://www.omnicoreagency.com/facebook-statistics/>.
- Ortiz-Ospina, E. (2019). Our world in data - the rise of social media. Accessed 24 June 2020. Available at: <https://ourworldindata.org/rise-of-social-media>.
- Rodrigues, A. A., Valentim, N. M. C., and Conte, T. (2017). Privacy evaluation of online social network stories feature: An empirical study with pdm. In *Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems, IHC 2017*, pages 1–10, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3160504.3160528.
- Social Media Perth (2021). Facts & figures // facebook statistics for 2022. Accessed 12 December 2021. Available at: <https://www.smp Perth.com/resources/facebook/facebook-statistics/>.
- Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3):477–560. DOI: 10.2307/40041279.
- Statista (2021). Facebook - statistics & facts. Accessed 12 December 2021. Available at: <https://www.statista.com/topics/751/facebook/>.
- Sundar, S. S., Kim, J., Rosson, M. B., and Molina, M. D. (2020). Online privacy heuristics that predict information disclosure. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, CHI '20*, page 1–12, New York, NY, USA. Association for Computing Machinery. DOI: 10.1145/3313831.3376854.
- Vincent, J. M., Bishop, F., Millard, D. E., and Stevenage, S. V. (2017). The cognitive heuristics behind disclosure decisions. In *Social Informatics. SocInfo 2017*, volume 10539, pages 591–607, Oxford, United Kingdom. Springer. DOI: 10.1007/978-3-319-67217-5_35.
- Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2):431–453. DOI: 10.1111/1540-4560.00072.
- Wu, H., Zhang, H., zhen Cui, L., and Wang, X. (2018). A heuristic model for supporting users' decision-making in privacy disclosure for recommendation. *Security and Communication Networks*, 2018:1–13. DOI: 10.1155/2018/2790373.
- Wu, P. (2018). The privacy paradox in the context of online social networking: A self-identity perspective: Journal of the association for information science and technology. *Journal of the Association for Information Science and Technology*, 70. DOI: 10.1002/asi.24113.
- Young, A. and Quan-Haase, A. (2013). Privacy protection strategies on facebook. *Information*, 16. DOI: 10.1080/1369118X.2013.777757.