sustainability

MDPI

Article

Digital Identity Management on Social Media: Exploring the Factors That Influence Personal Information Disclosure on Social Media

Joseph Kwame Adjei [1], Samuel Adams [2], Isaac Kofi Mensah [3,*], Peter Ebo Tobbin [1] and Solomon Odei-Appiah [1]

[1] School of Technology, Ghana Institute of Management and Public Administration (GIMPA), Accra 039 5028, Ghana; jadjei@gimpa.edu.gh (J.K.A.); ptobbin@gimpa.edu.gh (P.E.T.); sodei-appiah@gimpa.edu.gh (S.O.-A.)

[2] School of Public Services and Governance, Ghana Institute of Management and Public Administration (GIMPA), Accra 039 5028, Ghana; sadams@gimpa.edu.gh

[3] School of Economics and Management, Jiangxi University of Science and Technology, Ganzhou 330098, China

* Correspondence: isaackofimensah@jxust.edu.cn

Received: 3 September 2020; Accepted: 12 October 2020; Published: 30 November 2020

Abstract: A number of social media platforms have emerged as dominant medium for societal discourse, enabling significant user involvement in creation and shaping of social media contents. However, the phenomenon raises the challenge of digital identity management on such platforms in order to maintain reputations and ensure information privacy preservation. This study examined the factors that influence users' decision to disclose personal information on Social Media and their antecedents. We employed a mixed-methods approach based on analysis of data of 250 respondents from tertiary institutions in Ghana, and 8 focus group discussions comprising 86 participants. The results revealed a lack of user awareness and appreciation of the limitations of the privacy settings on social media platforms. Secondly, we observed that users' ability to establish the legitimacy of parties to social media interactions are fundamental requirements in how individuals engage social media. Finally, there is a disparity between information privacy concerns and actual privacy practices of users on social media.

Keywords: social media; autonomy; digital identity; self-determination; competence; Information Privacy

1. Introduction

In the last few years, social media has become part of the lives of people around the world. One of the most profound changes today is the increase in mobility of portable yet powerful wireless devices capable of communicating via several different kinds of wireless networks of varying link-level characteristics. The Internet and social media have become the most important achievement of modern society and particularly in Africa, they have helped to improve access to education, information technology, science and entertainment [1]. It is not surprising that the Global Digital Report (2019) describes social media as the ultimate representation of globalization. Social media continues to spread because its utility, and is supported by new trends and developments in technology and also by the improvement in knowledge and skills of social media users [2]. Nonetheless, as users enjoy the convenience offered by these platforms, service providers collect, analyse, and most often share personal information of users [3,4]. Accordingly, information security has become a critical issue in society and therefore a major topic in both research and practice [4,5].

About 50% of the world's nearly 3.80 billion population are social media users. Similarly, more than 5.19 billion people globally use mobile phones regularly, with user numbers up by 124 million (2.4 %) over the past year. The trend is similar across all the regions of the world. For example, out of the total population of 1.30 billion in Africa, 80 percent use mobile phones, and active social media users grew by 13 percent (25 million people). The use of social media on mobile devices also grew by 17 percent (30 million Africans) [6]. According to the report, Ghana has about six million active social media users and 20 million mobile phone users and ten million using the Internet. Though the level of development of Ghana is more than the average SSA country, citizens complain of economic hardships and lack of employment, but are able to raise the resources needed to purchase Internet data, smartphones, computers—to keep themselves active on the Internet, particularly social media. This has earned Ghana the 9th position globally in terms of hours spent on social media. Ghanaians spend considerably longer hours online than their African counterparts, which could mean that the West African nation spends significant amount of cash on Internet bundles for accessing social media. Social media users are offered tremendous opportunity to exercise informational self-determination [7], which seems to have contributed to the unprecedented adoption and use of social media by individuals and organizations. This has also been driven by the many expected benefits of social media, particularly the use of social media as a participatory and mobilizing platform for electoral democracy [8]. The 2016 presidential elections in Ghana attest to the growing power of social media, particularly Facebook, in inducing participation among potential voters.

The issue of security of identity even becomes more important when one considers the fact that the global digital growth shows no signs of slowing down, with about a million people around the world going online every day. This trend will continue because despite the problems of hacking, fake news and all other negative connotations associated with going online, around the globe people embrace the Internet because of the perceived social, political, and economic benefits [6]. This is especially the case for young adults who have different attitudes towards information security practices [9]. However, the requirement for the security of personal identity is not adequately met in networks, especially given the emergence of ubiquitous computing devices that are mobile and use wireless communications [10]. Although previous studies on social media have underscored its pivotal role in shaping interactions, the contextual factors in digital identity management on social media have not been well articulated. Digital identity is a keystone that can ensure that the Internet infrastructure is strong enough to meet basic expectations for not just service and functionality, but security, privacy, and reliability [11]. Personal information disclosure is one such digital identity issue that requires thorough interrogation. Shibuya [12] put it simply that digitized world requires identity protection. According to Pavlou [5], information privacy should be studied as a multi-level concept, as there are promising research directions for advancing the theme. Syd et al., [13] posited that given the paucity of research on identity management on social media, a value perspective is required to determine gaps between what social media users want and what social media sites offer through their current security and privacy controls [13]. Chang and Heo also note that while many social media studies have explored the degree to which social media users reveal their personal information, there has not been a systematic analysis of the factors that might explain users' self-disclosure on social media [14–16]. This gap motivates the study.

Obviously, the development of services and the growing demand for resources sharing among users from different organizations with some level of affinity have motivated the creation of Identity Management Systems [17]. As noted by Windley when it comes to enabling a truly virtual world that can accommodate the complexities of human behavior, nothing is more important than identity. Indeed, the network applications together with the ubiquitous connectivity to free transactions, communications, and other activities from physical constraints create a new set of requirements [18]. The purpose of this study is to explore the antecedents of personal information disclosure on social media. The central research question is, "What factors influence users' decision to disclose personal information on Social Media?" Addressing this question will effectively enrich current understanding of

the antecedents of personal information disclosure on social media and information privacy discourse in Information System research. It is expected that findings of the study could contribute to the extant literature on digital identity management and more importantly lead to evidence informed policy on social media to enhance its positive effects and possibly reduce negative impacts.

The rest of the paper are organized as follows: the next section provides an overview and conceptual foundations of social media. We then proceed to explain the concepts of identity and identity management and the major user concerns in their social media engagements including the theoretical lenses of the paper. The methodology and the results of the study are discussed respectively followed by conclusions and suggestions for further studies.

2. Background and Related Work

In this section a brief overview of the key concepts are discussed after which the theoretical and empirical literature are presented. The key concepts to be discussed are Social media, self-disclosure, and digital identity management.

2.1. Overview of Social Media

The technological advancements in mobile and Internet technologies have contributed to the phenomenal diffusion of user-friendly communication tools and social media platforms like Facebook, YouTube, WhatsApp, Twitter, WeChat, QQ, Pinterest, and Instagram [19]. Such platforms enable users to share content, opinions, and experiences and discuss issues they care about in the form of text, videos and pictures [20]. Social media, therefore, has departed from the initial idea of production and consumption and sharing of information to focus more on engagement and collaboration with clients [21]. Accordingly, Andzulis, Panagopoulos, and Rapp [22] define social media as "the technological component of the communication, transaction and relationship building functions of a business which leverages the network of customers and prospects to create value for all involved". Similarly, Boyd & Ellison define social media as "web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share connections and views, and traverse such list of connections and those made by others within the system" [23]. These definitions are more comprehensive than those that focus on social media simply as creating opportunities for companies to tell their stories to customers [24].

Harlow observed that social media technologies provide opportunity for real time user participation in societal discourse [25]. Social media innovation offers users a fast, easy and relatively cheap collection, aggregation and analysis of large volumes of data, with little or sometimes, no involvement of the data originator and/or the data subject [26,27]. Besides the relative ease of such interactions, better content, reach and richness, offer citizens the opportunity to contribute to various forms of discourse. The social media evolution began in 1995, with the emergence of a platform called Classmates [28]. Subsequently, social network platforms like Friendster, a dating platform, LinkedIn, a platform for managing users' professional identity emerged in 2003 and MySpace for content creation and sharing. Subsequently, Facebook that has become one of the dominant social media platforms emerged in the year 2004, followed by YouTube in 2005 and there have been several variations of social media innovations [29–31].

In Africa, the most popular social media platforms are Facebook (69.8%), YouTube (16.9), LinkedIn (1%), Pinterest (7.3%), Twitter (4.3%), and Instagram (0.9%) [6]. Though the trend is not very different in Ghana, there are slight variations. For example, though Facebook is the most popular, it is used by just about half of social media users (47%), 21% for Twitter, 18% for Pinterest, 10% for Instagram and 3.2% for YouTube [1,6]. In Africa more generally, and Ghana specifically, social media continues to spread because its utility is supported by new trends and developments in technology and because of the improvement in knowledge and skills of social media users. This is especially true as new and many forms of online content, platforms and websites continue to emerge for political communication and more importantly to improve the quality of governance [32,33]. It is worthy of mention that in a

few instances, social media has been used by some African governments to monitor and control their citizens so that instead of becoming a liberating force, it has become a conduit for surveillance and electoral manipulation [34–36].

The new social media platforms are redefining the way governments engage the citizenry, per its influence on the perceptions, views and actions of individuals whose opinions have traditionally been influenced by information from traditional forms of media [35,37] lso, of value are the concerns of civil society for a regulatory framework to guide the use of social media before, during and after elections to curb the propagation of fake news or unsubstantiated information on these platforms. In sum, it can be argued that social media could offer opportunities for innovation and entrepreneurship that help to simplify complex relationships because of the ease and fastness with which data could be collected and analysed [26,27,38]. Alongside the relative ease of such interactions, better content, reach and richness, social media offer citizens the opportunity to contribute to various forms of discourse in real time, where they are limited or are no longer hostages to geography [39].

2.2. Self Disclosure

On the whole, social media like most things in life have both benefits and risks and one of the basic challenges confronting users of the several social media platforms is how to protect their privacy and consequently how much they could disclose of themselves online. Many theoretical frameworks have been used to explain the factors that drive self-disclosure including the self-determination theory, social contract theory, social exchange theory and the uses and gratification theory. In essence, self-disclosure refers to the communication behavior in which an individual wilfully reveals himself to others [40]. Revealing themselves in this sense involves their thoughts, feelings and experiences which help to maintain online social networks [41]. From this perspective, it is important to state that self-disclosure not only helps to initiate social interactions, but also facilitates richer social contacts and friendships in the long-term [42].

The question is what are the factors that drive these behaviors to disclose or otherwise? Consistent with the social contract and social exchange theories, the decision to disclose or otherwise is perceived through a cost—benefit analysis where a net benefit leads to disclosure and a net cost leads to withdrawal or non-disclosure [43,44]. Obviously, the decision would be based on the perceived risk or benefit associated with disclosure. Some empirical studies indicate that people are attracted to those who grant them rewards when initiating interpersonal contact on Internet dating sites or perceive more benefits than risks are more likely to disclose personal information [45,46]. This supports the view of Zhang et al. (2019) that self-disclosure is usually driven by the estimation of costs and benefits between parties in the relationship. Also, the relationship between privacy attitudes and self-disclosure behaviors has largely been explained by the notion that individuals regulate their exchange of information based on privacy control mechanisms [47,48]. More intriguing is the fact that self-disclosure not only helps to initiate social interactions, but also facilitates richer social contacts and friendships in the long-term [42]. Thus, the very survival and quality of many of the social media platforms is determined by the level of disclosure.

Other complementary theories that could be used to explain self-disclosure phenomenon are the theories of reasoned action, planned behavior, and uses and gratifications theory. These theoretical perspectives generally seem to suggest that the decision to disclose is dependent on the individual's own perceived value of the decision, which determines the intention whether to take action or not. As indicated by the theory of reasoned action, intention influences, which supposes that the effort towards an activity to achieve a particular behavioral outcome is determined by the intention one [49]. In recent times, the theory of reasoned action has been complemented with the theory of plans behavior, which claims that the intention toward attitude, subjective norms, and perceived control, together shape an individual's behavioral intentions and the subsequent actual behaviors exhibited or executed. That is to say that the stronger the intention the more likely the behavior will be executed [4,49,50]. The views expressed are also consistent with the uses and gratifications theory (U&G) thesis that

explains that people are generally goal driven and this motive influences their media use and other outcomes, such as attitude and behavioral intentions [51]. In sum, the U&G theory assumes that people always take actions that will lead to the fulfilment of certain gratifications. As noted by Chang and Heo different motives lead to the disclosure of different types of personal information, which echoes U&G's assumption that users tend to use media in different ways to fulfil their diverse needs [14].

The underlying principle of all the theories discussed is the idea of trust, which many authors suggest has the most important influence on information disclosure [52–55]. This is understandable because of not only the extensive use, but more importantly the impersonal nature and the uncertainty of open Internet [53]. This is supportive of Yu et al.'s finding that perceived privacy risks of users have stronger negative impact on disclosure intention and behavior on instrumental platforms, compared with emotional platforms [4]. Many studies also do show that the biggest constraint to the growth of social media is the issue of trust or the public's fear about security and privacy online [16]. Some others also report that trust has the most important influence on information disclosure [53,54]. Indeed, several studies of interpersonal exchange situations have confirmed that trust is a precondition for self-disclosure because it reduces the perceived risks involved in revealing private information [56–59].

In effect, what is being disclosed is the identity of the user of the social media, which refers to the qualities and characteristics that make an entity definable, distinguishable, and recognizable compared to other entities [60]. Or as Bellini et al. [11] describe it, identity consists of a set of information associated with a specific entity and it is usually a reflection of what is generally known by those with whom they interact [61]. That entity or agent may be a person or individual, organization, application, or device that exists online. Additionally, Bellini et al. observe that when it comes to enabling the virtual world, nothing is more important than identity in explaining the depth of human behavior [11]. Identity management therefore becomes the cornerstone of Internet infrastructure to ensure that not only expectations are being met in terms of service and functionality but also security, privacy, and reliability. Identity in the digital world is digital records that represent a user which are usually saved and managed in a standard format by entities that provide those identity information. The concept of identity is therefore vital in the formation of better knowledge of people and in trust building, since it provides the foundation for socio-economic interactions. Such definitions have widened the concept of identity to include identifiers such as login names and pseudonyms. Identity in information systems therefore consists of peculiar traits, attributes, and preferences that used to provide personalized services to users [62]. Such tweets, posts, likes, email trails or tags produce a digital footprint that can be connected perpetually to users digital identity [63]. Such digital footprints usually released during user interactions and exchanges on social media are sometimes referred to as digital personas or partial identity, as illustrated in Figure 1 [64].

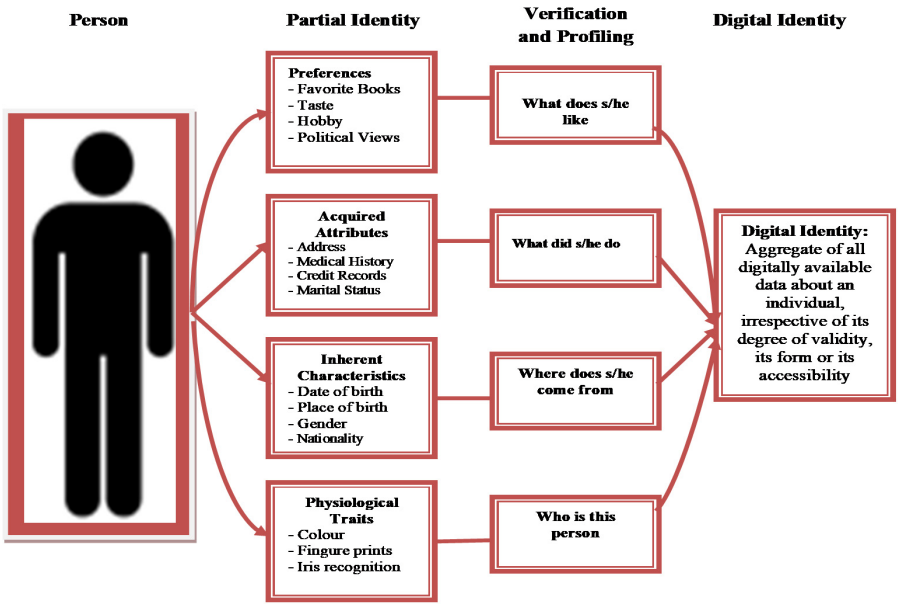

Figure 1. Digital Persona or Partial Identity.

The diagram (Figure 1) clearly shows that the sets of identity attributes and identifiers used for specific transactions on the Internet may vary considerably depending on the context [65]. Effective identification is therefore, based on users' ability to demonstrate knowledge (something you know—e.g., a password); possession of a token or credential (something you have—e.g., driver's license); physiological characteristics or features (something you are—e.g., gender, facial features, signature, fingerprint), or a combination of all or any of the three [66,67].

2.3. Digital Identity Management

The architecture of the Internet allows users to disguise their digital persona resulting in the quest for reliable means of ascertaining identities with certainty [68]. To ensure that data subjects are unmistakably identifiable, identity tokens must be tamper resistant, or difficult to forge after they are issued. Digital identity therefore, removes the requirement for parties to be present during transactions and interactions. Such a disembodiment of identification processes results in wider distribution of personal information [69]. Cameron proposed the laws of identity as design principles (Table 1), that should form the foundation for constructing the identity [68]. The paper posited that adherence to such principles offers user control and the ability to influence how their personal information is used for secondary purposes. Non-conformance to such design principles raises user concerns which can influence their engagement on social media.

2.4. User Concerns on Social Media

Various sophisticated tools enable users to collect, aggregate and analyse large volumes of personal information on social media. Chatzakou et al., for instance, proposed a machine learning-based detection model to identify multiple virtual identities of the same natural person [70]. Such innovations are usually intended to enhance the notion of self-presentation and informational self-determination. In spite of such unprecedented sophistication, various studies have explored the risks associated with personal information disclosure on social media [71]. Such legitimate user concerns often hinder information disclosure on social media, compelling users to constantly examine their natural quest for connectivity and user experience, and a requirement to disclose sensitive information. Moreover, although users rely on a variety of cues in determining how to connect and interact with others on social media, not all of such cues are credible because the architecture of the Internet makes it difficult

to know with certainty, the identity of interacting parties. This is because users observed behavior on social media platforms are usually different from what is stated [72].

Table 1. The Laws of Identity (Cameron, 2005).

Principe	Brief Description
User Control and Consent	Technical identity systems must only reveal information identifying a user with the user's consent.
Minimal Disclosure for a Constrained Use	Digital Identity solutions that disclose the least amount of identifying information and best limit its use is the most stable long-term solution.
Justifiable Parties	Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
Directed Identity	A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles
Pluralism of Operators and Technologies	A universal identity system must channel and enable the inter-working of multiple identity technologies operated by multiple identity providers.
Human Integration	Digital identity systems must define the human user as a component of the distributed system and offer protection against identity attacks.
Consistent Experience Across Contexts	Users must be guaranteed simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Altman conceptualized privacy in relation to how individuals regulate access to themselves, and Culnan and Stewart & Segars described privacy concerns as the extent to which individuals are disturbed about the information collection practices of others and how the acquired information will be used [47,73,74]. Hurwitz posited that decisions to disclose personal information on social media hinges on individual sensitivities towards what is perceived as privacy invasion [75]. Thus, concerns about possible loss of privacy as a result of personal information disclosure to third parties is what underpins privacy concerns [76,77].

3. Conceptual Framework

According to the self-determination theory (SDT), needs are the most important determinants of human behavior [78]. As noted by Deci and Ryan, the main aim of human behaviors is to satisfy the basic psychological needs throughout the lifetime. In a sense, SDT links human motivation, personality, and the actual functioning of an individual [78,79]. The SDT therefore provides a unique perspective to examine the relationship between peoples' needs and their social media behavior [80]. Primarily, the SDT is centered on the fundamental humanistic assumption that individuals naturally seek growth and self-organization [81]. Shen et al. describe the psychological needs as the innate psychological nutrients essential for ongoing growth, integrity, and well–being [80]. Deci and Ryan's SDT identifies three basic psychological needs as competence, relatedness, and autonomy. These three elements when satisfied yield enhanced self-motivation and mental health and when thwarted lead to diminished motivation and well-being [82].

Competence is the ability to control the outcome of an activity and experience mastery of that task, which relates to the need to perform successful social interactions with skills and ability. Relatedness is associated with the universal need to be connected to an experience caring for others and autonomy refers to the need to decide one's own behavior and act freely in accordance with their interests and beliefs [7,78,83]. For example, autonomy entails ability to act with a sense of volition and having the experience of choice. Accordingly, in social media engagements, individuals must have the ability to prevent sensitive information from one context (e.g., the employment data, medical records, relationships) from proliferating into other platforms. The information disclosure behavior on social media is therefore, a function of users' ability to evaluate the specific risks and benefits of the online

transaction [84]. Many studies do provide support for these psychological needs, digital literacy skills and self-information disclosure. For example, Boyd & Hargittai report that Internet users with high level of skills update their privacy settings more frequently, whereas the reverse is reported for those with minimal skills [29,85]. Demirbaş-Çelik and Keklik in a study of high school students in Turkey report that each psychological need (competence, relatedness and autonomy) partially mediated the relationship between stability and presence of meaning in life [86]. On the other hand, only competence and relatedness partially mediated the relationship between plasticity and search of meaning [83]. The findings suggest that competent users are more likely to self-determine how their personal information is used on social media. Similarly, Demirbas-Celik examines the roles of the satisfaction of basic psychological needs and meaning in life (MIL) on high school students' happiness and demonstrate that autonomy, competence, relatedness and MIL predict social well-being significantly [86]. In a related study, Martela et al. found that competence, relatedness, autonomy and beneficence each independently accounted for variance in MIL [87]. Likewise, Weinstein et al. reported a link between psychological needs and meaning in life [88].

Figure 2 provides a pictorial representation of the self-determination theory. The cardinality of autonomy, relatedness and competence in personal information disclosure behavior on social media show that, individuals will disclose personal information if they possess understanding of the platform. The disclosure is a means to show intimacy and relatedness, or the user is not under duress to disclose personal information.

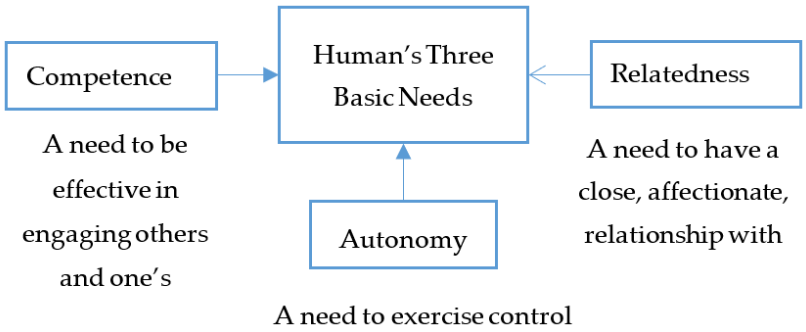

Figure 2. Informational Self-Determination [78].

Moreover, Hoffmann et al. identified a cognitive coping mechanism that enables users to overcome or ignore privacy concerns and engage in online information self-disclosure [89]. Also the integrity and openness of social media platform can influence users' information disclosure behavior [90]. Trust of social media platforms is therefore predicated on integrity and openness. We therefore argue that, the key factors that influence personal information disclosure on social media are: competence, relatedness, autonomy, integrity and awareness of the risks and its consequence as illustrated in Figure 3. The methodology employed to achieve the research objectives are described next.

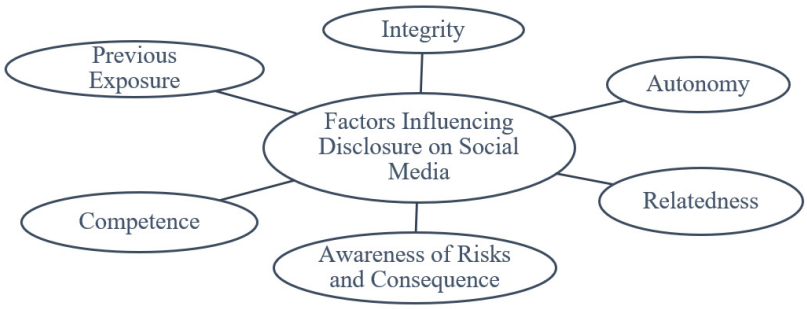

Figure 3. Factors Influencing Information Disclosure on Social Media.

4. Methods

A variation of convergent parallel mixed methods design was adopted in this study to explore the factors that influence personal information disclosure on social media. This method is suitable for developing a complete understanding and a comprehensive view of the research domain and the research problem [91]. This research design involves a concurrent use of quantitative and qualitative elements in the research processes, independent analysis of the two components, and joint interpretations of the results [91,92]. The quantitative strand involved a convenient sample of two hundred and fifty (250) students from tertiary institutions in Ghana who completed a carefully designed instrument. Respondents provided biographic data and were required to select personal information attributes they were willing to disclose on a social media. Given the validation issues with respect to the limited number of respondents, the qualitative analysis was carefully designed to provide rich explanations of the findings from the quantitative data and analysis [93,94].

With respect to the qualitative strand of the study, Venkatesh et al. specified six types of social network analysis for which qualitative research methods will be suitable. Such social media analytical categories include; exploration of networks, examination of network practices, network interpretations, network effects, network dynamics and access to actors and networks [93,94]. The qualitative analysis is therefore justified since this study examines user behavior and practices on social media [93,94]. Eighty-six (86) students (both undergraduate and graduate) participated in the eight focus group discussions. A purposive sampling technique was adopted in the nomination of the participants of the focus group. The age groups and gender were carefully considered in the formation of the focus groups to encourage frank and open discussion of the issues raised (See Table 2).

Table 2. Summary of Users' Perceptions and Attitudes.

Focus Group	Venue	Number of Participants	Composition		Age Group	Summary of Findings
			Males	Females		
1	GIMPA	10	6	4	20–25	Users with prior exposure are very cautious of what they post on social media. Attention seeking users are usually not information privacy sensitive.
2	GIMPA	12	5	7	22–35	Information sharing with close relatives and friends are usually with less precaution.
3	KNUST	8	5	3	19–26	Users who are competent on social media usually exercise less precaution. Such users are very selective in the use of the privacy settings.
4	U.G	11	7	5	18–27	There is a disparity between information privacy concerns and actual practices on social media.
5	U.G	10	4	6	19–25	The actual user disclosure behavior on social media is usually different from their disclosure intentions.
6	U.G	12	4	6	18–28	Perceptions and attitudes of relatives and friends affect users behavior on social media
7	GIMPA	11	7	5	20–33	Pseudonyms are used to create a mask between users' online and physical behavior.
8	KNUST	12	8	4	18–30	Many users believe that pseudonyms allow them to hide their true identity on social media.
Total Participants		86	46	40		

Prior to each of the focus group discussions, participants were briefed on digital identity management and information disclosure issues on social media. The discussion covered the issues that participants take into consideration in their social media engagements and disclosure behaviors. Participants' previous exposure, computing and social media proficiency and the benefits derived were also discussed. Responses to the questions generated probing questions from the researcher and occasionally, members of the focus group. All the focus group discussions took place in the last quarter of the year 2019. The discussions were recorded, and data were transcribed unto a Microsoft Word document. Content analysis was adopted for the focus group data analyses. The transcribed data were categorized using open coding technique for classification and tabulation into common themes as illustrated in Figure 3.

5. Discussion of Results

The study explored the factors that contribute to personal information disclosure on social media. Figure 4 is a summary of information that the respondents were willing to disclose on social media and what they were less willing to disclose on social media.

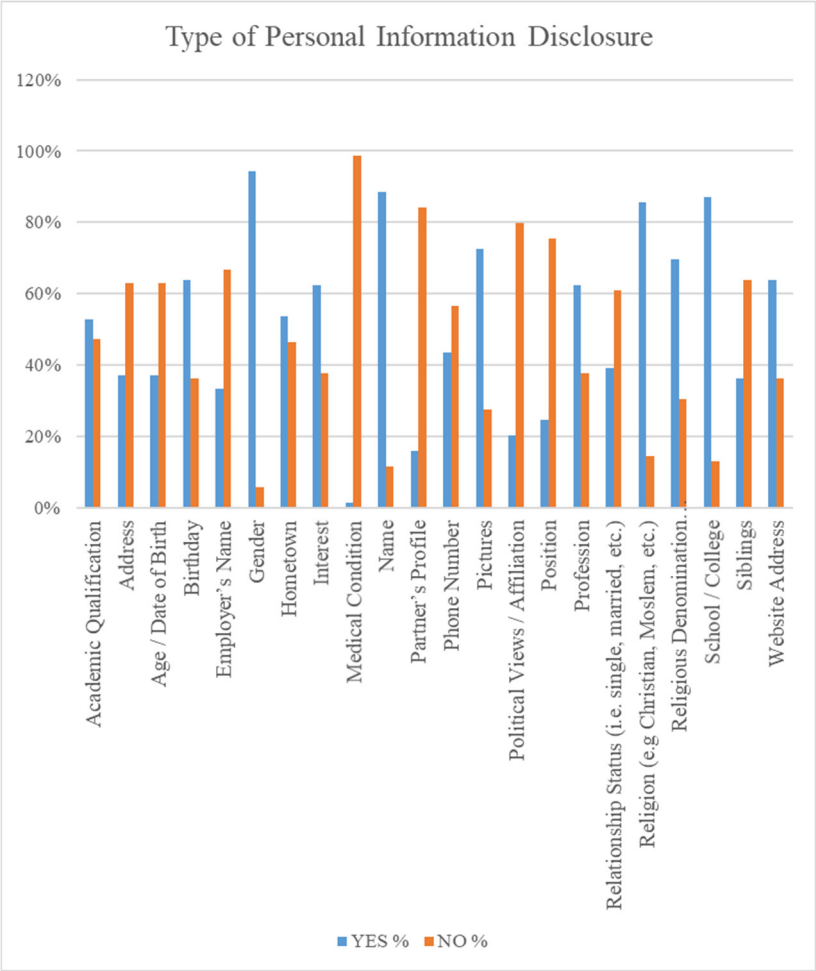

Figure 4. Determinants of Personal Information Disclosure.

The survey revealed some interesting results. The respondents were almost unanimous in their disclosure intentions on medical history. Only about two percent of the respondents were willing to disclose their medical information on social media. This provides a clear indication of users' unwillingness to compromise on their medical records. Similarly, 90% of the respondents were unwilling to disclose their partner's profile. We also noted a disparity in the intention to disclose

personal information, and the choice of media based on gender. For instance, female users are more willing to display their pictures (76%) on social media than their male counterparts (62%). Majority of the female respondents preferred Facebook, Instagram and Snapchat as their preferred Social Media Application. Interestingly, majority of the respondents who preferred Twitter and LinkedIn were males. There were some disparities in user attitudes on social media based on the age group. Respondents aged 25 and below were more willing to disclose sensitive information like phone numbers (76%), address (72%), whereas those above 25 years were more open about their political views on social media (64%).

Remarkably, glancing through Facebook accounts of many of the respondents revealed their family photos, wedding pictures and birthday wishes to partners that clearly provide indication of the nature of relationship. Similarly, phone numbers of many of the respondents were disclosed on social media although about 60% had indicated their unwillingness to disclose phone numbers indicating a mismatch between user intentions and actual behavior on social media. Responses from the eight (8) focus group discussions provided deeper insights into users' information disclosure behaviors. For instance, it revealed a lack of awareness and appreciation of the limitations of the privacy settings of social media platforms and their implications which are revealed in comments like, "I prefer simple privacy settings like that of Whatsapp" I usually don't go to the complicated settings". Clearly, simple privacy settings may not address many of the privacy concerns, whereas elaborate privacy settings like that of Facebook may be too complicated for users creating the so called "privacy dilemma."

Moreover, analysis of focus group data indicated a correlation between previous exposure and disclosure behavior of the respondents as confirmed by the following statements:

> *"My father used my posts on Instagram to detect a guy I was dating, it was not easy for me. Since I posted a video of a school party on Facebook, some of my relatives have accused me of being a spoilt child so I have deleted such videos from my account a certain guy started sending me suggestive pictures and even tried to blackmail me into sleeping with him. Apparently, he found my contact details on Facebook. I have since deleted my contact details and changed my cell phone number. These days I only share information with only those I know. I do not make them public."*

These are clear indications that, those who have had episodes of information abuse were less willing to disclose certain information on social media. Moreover, those who appreciate the consequences of the exposure will be less willing to disclose even their names and personally identifiable information. In such situations, pseudonyms were used to conceal their true identity as indicated in the following comments:

> *"I usually to use nicknames on social media instead of my actual name. Even some of my close relatives do not know my Facebook account" some of my friends do not know that I am very active on social media because I do not post picture". "I only share birthday and party photos with friends on social media using nicknames."*

Interestingly such respondents also complained about wrong people being suggested to them by social media platforms. Participants' awareness of risks and the consequences of the risk influence how they engage on social media. For instance, a participant hinted that

> *"I suspect that what I say on social media and the type of friends that I engage with on social media can affect my chances of getting a visa to certain countries". I have noticed that whenever I change my photo on LinkedIn, the system suggest friends with similar features to me. I am forced to change my picture of LinkedIn because I suspect potential employers might not take me seriously."*

The study has revealed that relatedness of users, integrity of users on the platform and competence of users are the key antecedents to privacy concerns on social media. In other words, perception of lack of integrity and low user competence have the tendency to lower the level of the trustworthiness of users [90]. Similarly, previous exposures and relationships can influence their trustworthiness.

Figure 5 clearly shows that relatedness, integrity and competence influence privacy concerns, which then informs the behavioral intention of individuals on social media and consequently, their actual social media engagements with respect to information disclosure.

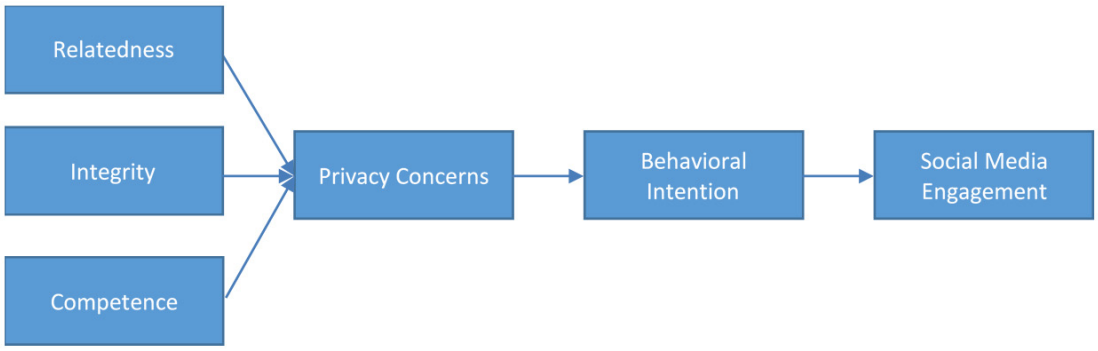

Figure 5. Personal Information Disclosure Model.

The results also provided an interesting revelation about the disclosure behavior of users and the benefits derived, which is consistent with the idea that human needs traditionally are key determinants of human behavior [83,95]. As noted by the self-determination theory, relatedness, competence and autonomy are not only innate but that being able to satisfy them are critical for proper functioning and well-being [82,86]. On the other hand, when these three are not satisfied, it might lead to inaction or inertia, maladjustment and psychopathological symptoms [96]. Relating this to the social media engagement, the behavioral intention to self-disclose or not to disclose per one's privacy concerns are determined by how close a person is to achieving the optimal psychological state as it concerns relatedness, integrity, and competence.

The assumption is that satisfaction of these three basic psychological Personality Factors and Meaning in Life determine whether to engage or not to engage, and to disclose or not disclose personal information on social media. In support of the theory of reasoned action and planned behavior, Mouakket and Sun find that an individual's subjective norms have a significant impact on the desire to self-disclose personal information on social network systems in China. For instance, respondents who conduct business activities on social media often disclose their individual and organizational contact details [97]. Such users are usually very competent on social media, and have had extensive exposure on social media which seems to have raised their level of trustworthiness in such platforms. We therefore argue that users' ability to establish the legitimacy of parties to social media interactions are fundamental requirements in how individuals engage on social media.

6. Conclusions and Further Work

The emergence of social media platforms as primary medium for societal discourse is increasingly raising digital identity management challenges like information privacy preservation and maintenance of user reputation. This study explored the key factors that influence how users engage on social media platforms and their information disclosure behaviors through the lenses of information privacy and self-determination theories. The results provided interesting revelations that contribute to existing understanding on digital identity management on social media, and factors that influence social media platform design. For instance, we identified a disparity between information privacy concerns and actual privacy practices on social media. For instance, users who claim non-disclosure of sensitive personal information on social media, usually do so using pseudonyms, whereas attention- seeking users are less information privacy sensitive on social media.

Theoretically, this study enhances existing understanding of how users engage on social media. The study has also shown that competence and user exposure positively influence personal information disclosure behavior. We, therefore, argue that users' ability to establish the legitimacy of parties to social media interactions are fundamental requirements in how individuals engage on social media.

The study has also deepened existing understanding of the information privacy calculus and their implications on information disclosure behaviors on social media by highlighting that competent users are likely to be selective in their use of the privacy settings on social media platforms. Thus, social media platform developers must improve the ease of the privacy settings to ensure a positive information disclosure behavior by social media users.

We note the validity issues in the use of two hundred and fifty (250) respondents in the quantitative strand of the study. However, adoption of mixed methods research design particularly addresses such limitations since inferences from the eight (8) focus group discussions comprising eighty-six (86) participants is intended to bridge the validation gap [93,94]. It is our expectation that future studies using extensive collection of data will be carried out to validate the findings from this study.

Future research should explore the relationships between the identified factors and the extent of their impact on personal information disclosure behavior of users using quantitative research techniques. Obviously, since most of the factors are latent behavioral characteristics, SEM techniques could be employed to identify the causal and dynamic relationship between the variables. Additionally, future studies should seek to conduct longitudinal studies to provide results that are more robust and yield more efficient and consistent estimates to give evidence to inform policy on digital identity management and education. This is particularly important in light of the fact that in recent years Africa has seen the world's highest Internet penetration growth rates. This means that we should expect social media to play an increasingly prominent role in the socioeconomic, political, cultural and security on the continent. Accordingly, any study that helps to shed light on these issues is in the right direction.

Author Contributions: Conceptualization, J.K.A.; Background and Related Work, J.K.A., S.A., I.K.M., P.E.T., S.O.-A.; Conceptual Framework, J.K.A., S.A., I.K.M., P.E.T.; Methods, J.K.A., S.A., I.K.M., P.E.T., S.O.-A.; Discussion of Results, J.K.A., S.A., I.K.M., P.E.T., S.O.-A.; Conclusions, J.K.A., S.A.; Writing—Original Draft Preparation, J.K.A., S.A.; Writing—Review and Editing, J.K.A., S.A., I.K.M., P.E.T., S.O.-A. All authors have read and agreed to the published version of the manuscript.

Funding: The work was not funded by any organization.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mohale, G.T. The Implications of Social Media Use on Development in Africa: A Development Theory Perspective. *Glob. J. Manag. Bus. Res.* **2020**, *20*, 63–72. [CrossRef]
2. Frøyen, I.W. Sometimes It's Not a Switch, It'sa Dial: An Analysis of the Genderqueer Narrative in Symptoms of Being Human, and the Effects of Genderqueer Representation in Young Adult Literature. Master's Thesis, University of Oslo, Oslo, Norway, 2019.
3. Li, H.; Luo, X.R.; Zhang, J.; Xu, H. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Inf. Manag.* **2017**, *54*, 1012–1022. [CrossRef]
4. Yu, L.; Li, H.; He, W.; Wang, F.-K.; Jiao, S. A meta-analysis to explore privacy cognition and information disclosure of internet users. *Int. J. Inf. Manag.* **2020**, *51*, 102015. [CrossRef]
5. Pavlou, P.A. State of the Information Privacy Literature: Where are We Now and Where Should We Go? *MIS Q.* **2011**, *35*, 977. [CrossRef]
6. Kemp, S. The Global State of Digital in October 2019. We Are Social. 2019. Available online: https://wearesocial.com/blog/2019/10/the-global-state-of-digital-in-october-2019 (accessed on 15 July 2020).
7. Gagné, M.; Deci, E.L. Self-determination theory and work motivation. *J. Organ. Behav.* **2005**, *26*, 331–362. [CrossRef]
8. Dzisah, W.S. Social Media and Participation in Ghana's 2016 Elections. In *Social Media and Elections in Africa*; Ndlela, M., Mano, W., Eds.; Palgrave Macmillan: Cham, Switzerland, 2020; Volume 1, pp. 97–118.
9. Yoon, C.; Hwang, J.W.; Kim, R. Exploring factors that influence students' behaviors in information security. *J. Inf. Syst. Educ.* **2019**, *23*, 7.

10. Mahalle, P.; Babar, S.; Prasad, N.R.; Prasad, R. Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges. In *Recent Trends in Network Security and Applications. CNSA 2010. Communications in Computer and Information Science*; Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; Volume 89. [CrossRef]
11. Bellini, F.; D'Ascenzo, F.; Dulskaia, I.; Savastano, M. Digital Identity: A Case Study of the ProCIDA Project. In *Exploring Digital Ecosystems*; Lazazzara, A., Ricciardi, F., Za, S., Eds.; Springer: Cham, Switzerland, 2020; pp. 315–327.
12. Shibuya, K. Identity Protection. In *Digital Transformation of Identity in the Age of Artificial Intelligence*; Shibuya, K., Ed.; Springer: Singapore, 2020; pp. 73–88.
13. Syed, R.; Dhillon, G.; Merrick, J. The Identity Management Value Model: A Design Science Approach to Assess Value Gaps on Social Media. *Decis. Sci.* **2018**, *50*, 498–536. [CrossRef]
14. Chang, C.-W.; Heo, J. Visiting theories that predict college students' self-disclosure on Facebook. *Comput. Hum. Behav.* **2014**, *30*, 79–86. [CrossRef]
15. Joinson, A.N.; Reips, U.-D.; Buchanan, T.; Schofield, C.B.P. Privacy, Trust, and Self-Disclosure Online. *Hum. Comput. Interact.* **2010**, *25*, 1–24. [CrossRef]
16. Metzger, M.J. Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *J. Comput. Commun.* **2006**, *9*, JCMC942. [CrossRef]
17. Haddouti, S.E.; Kettani, M.D.E.C.E. Towards an interoperable identity management framework: A comparative study. *arXiv* **2019**, arXiv:1902.11184.
18. Windley, P.J. *Digital Identity: Unmasking identity management architecture (IMA)*; Springer: Berlin, Germany, 2005; p. 52.
19. Statista. Global Social Media Ranking 2018. Statistic. Statista. 2018. Available online: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (accessed on 20 August 2020).
20. Tsay-Vogel, M.; Shanahan, J.; Signorielli, N. Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media Soc.* **2016**, *20*, 141–161. [CrossRef]
21. Cao, J.; Basoglu, K.A.; Sheng, H.; Lowry, P.B. A systematic review of social networking research in information systems. *Commun. Assoc. Inf. Syst.* **2015**, *36*, 727–758.
22. Andzulis, J.M.; Panagopoulos, N.G.; Rapp, A. A Review of Social Media and Implications for the Sales Process. *J. Pers. Sell. Sales Manag.* **2012**, *32*, 305–316. [CrossRef]
23. Boyd, D.M.; Ellison, N.B. Social Network Sites: Definition, History, and Scholarship. *J. Comput. Commun.* **2007**, *13*, 210–230. [CrossRef]
24. Ploof, R. Johnson & Johnson Does New Media. 2009. Available online: http://ronamok.com/ebooks/jnj_case_study$\blacksquare$pdf (accessed on 20 August 2020).
25. Harlow, S. Social media and social movements: Facebook and an online Guatemalan justice movement that moved offline. *New Media Soc.* **2011**, *14*, 225–243. [CrossRef]
26. Bélanger, F.; Crossler, R.E. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Q.* **2011**, *35*, 1017–1042. [CrossRef]
27. Malhotra, N.K.; Kim, S.S.; Agarwal, J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Inf. Syst. Res.* **2004**, *15*, 336–355. [CrossRef]
28. Sajithra, K.; Patil, R. Social Media—History and Components. *J. Bus. Manag.* **2013**, *7*, 69–74. [CrossRef]
29. Boyd, D.; Ellison, N.B. Social network sites: Definition, history, and scholarship. *IEEE Eng. Manag. Rev.* **2010**, *38*, 16–31. [CrossRef]
30. Leader-Chivee, L.; Hamilton, B.A.; Cowan, E. Networking the way to success: Online social networks for workplace and competitive advantage. *People Strategy* **2008**, *31*, 40.
31. Neumann, M.; O'Murchu, I.; Breslin, J.; Decker, S.; Hogan, D.; Macdonaill, C. Semantic social network portal for collaborative online communities. *J. Eur. Ind. Train.* **2005**, *29*, 472–487. [CrossRef]
32. Asongu, S.A.; Le Roux, S.; Nwachukwu, J.C.; Pyke, C. The mobile phone as an argument for good governance in sub-Saharan Africa. *Inf. Technol. People* **2019**, *32*, 897–920. [CrossRef]
33. Boateng, A.B.; McCracken, D.P.; Lubombo, M. Intra-Party Election Campaigns in Ghana: An Analysis of Facebook Use. In *Social Media and Elections in Africa*; Ndlela, M., Mano, W., Eds.; Palgrave Macmillan: Cham, Switzerland, 2020; Volume 1, pp. 215–232.
34. Shahbaz, A.; Funk, A. *Freedom on the Net*; The Crisis of Social Media; Freedom House: Washington, DC, USA, 2019.

35. Dwyer, M.; Molony, T. Analysis across Africa Shows How Social Media is Changing Politics. 2019. Available online: https://theconversation.com/analysis-across-africa-shows-how-social-media-is-changing-politics-121577 (accessed on 16 August 2020).
36. Ndlela, M.N.; Mano, W. (Eds.) The Changing Face of Election Campaigning in Africa. In *Social Media and Elections in Africa*; Palgrave Macmillan: Cham, Switzerland, 2020; Volume 1, pp. 1–12.
37. Kamp, M. (Ed.) *Assessing the Impact of Social Media on Political Communication and Civic Engagement in Uganda*; Uganda Programme, Konrad Adenauer-Stiftung: Kampala, Uganda, 2016; Available online: http://www.kas.de/wf/doc/kas_43976-1522-2-30.pdf?160125084552/ (accessed on 20 August 2020).
38. Ratten, V. Social media innovations and creativity. In *Revolution of Innovation Management*; Brem, A., Viardot, E., Eds.; Palgrave Macmillan: London, UK, 2017; pp. 199–220.
39. Hamel, G.; Sampler, J. The e-Corporation. *Fortune* **1998**, *138*, 80–87.
40. Derlega, V.J.; Berg, J.H. *Perspectives in Social Psychology. Self-Disclosure: Theory, Research, and Therapy*; Plenum Press: New York, NY, USA, 1987; Available online: https://www.springer.com/gp/book/9780306426353 (accessed on 20 August 2020).
41. Zhang, S.; Kwok, R.C.-W.; Lowry, P.B.; Liu, Z. Does more accessibility lead to more disclosure? Exploring the influence of information accessibility on self-disclosure in online social networks. *Inf. Technol. People* **2019**, *32*, 754–780. [CrossRef]
42. Nosko, A.; Wood, E.; Molema, S. All about me: Disclosure in online social networking profiles: The case of Facebook. *Comput. Hum. Behav.* **2010**, *26*, 406–418. [CrossRef]
43. Fishbein, M.; Ajzen, I. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*; Addison-Wesley: Reading, MA, USA, 1975.
44. Kankanhalli, A.; Tan, B.C.Y.; Wei, K.-K. Contributing knowledge to electronic knowledge repositories: An empirical investigation. *MIS Q.* **2005**, *29*, 113–144. [CrossRef]
45. Shtatfeld, R.; Barak, A. Factors related to initiating interpersonal contacts on Internet dating sites: A view from the social exchange theory. *Interpersona Int. J. Pers. Relatsh.* **2009**, *3*, 19–37. [CrossRef]
46. Krasnova, H.; Spiekermann, S.; Koroleva, K.; Hildebrand, T. Online social networks: Why we disclose. *J. Inf. Technol.* **2010**, *25*, 109–125. [CrossRef]
47. Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*; Brooks/Cole Publishing Company: Monterey, CA, USA, 1975.
48. Petronio, S. *Boundaries of Privacy: Dialectics of Disclosure (SUNY Series in Communication Studies.)*; State University of New York Press: New York, NY, USA, 2002; p. 6.
49. Ajzen, I.; Fishbein, M. Attitudinal and normative variables as predictors of specific behavior. *J. Personal. Soc. Psychol.* **1973**, *27*, 41. [CrossRef]
50. Ajzen, I. (Ed.) From intentions to actions: A theory of planned behavior. In *Action Control*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 11–39.
51. Katz, E.; Blumler, J.G.; Gurevitch, M. Uses and gratifications research. *Public Opin. Q.* **1973**, *37*, 509–523. [CrossRef]
52. Hoffman, D.L.; Novak, T.P.; Peralta, M.A. Information privacy in the marketspace: Implications for the commercial uses of anonymity on the Web. *Inf. Soc.* **1999**, *15*, 129–139.
53. Jarvenpaa, S.L.; Tractinsky, N.; Saarinen, L. Consumer trust in an Internet store: A cross-cultural validation. *J. Comput. Mediat. Commun.* **1999**, *526*, 5. [CrossRef]
54. Jarvenpaa, S.L.; Staples, D.S. The use of collaborative electronic media for information sharing: An exploratory study of determinants. *J. Strateg. Inf. Syst.* **2000**, *9*, 129–154. [CrossRef]
55. Swaminathan, V.; Lepkowska-White, E.; Rao, B.P. Browsers or buyers in cyberspace? An investigation of factors influencing electronic exchange. *J. Comput. Mediat. Commun.* **1999**. [CrossRef]
56. Jourard, S.M. *The Transparent Self*; Van Nostrand Reinhold Company: New York, NY, USA, 1971; ISBN 0-442-24192-5.
57. Rubin, Z. Disclosing oneself to a stranger: Reciprocity and its limits. *J. Exp. Soc. Psychol.* **1975**, *11*, 233–260. [CrossRef]
58. Steel, J.L. Interpersonal correlates of trust and self-disclosure. *Psychol. Rep.* **1991**, *68*, 1319–1320. [CrossRef]
59. Wheeless, L.R.; Grotz, J. The measurement of trust and its relationship to self-disclosure. *Hum. Commun. Res.* **1977**, *3*, 250–257. [CrossRef]
60. Ayed, G.B. *Architecting User-Centric Privacy-as-a-Set-of-Services: Digital Identity-Related Privacy Framework*; Springer: Geneva, Switzerland, 2014.

61. Wilton, R. Identity and privacy in the digital age. *Int. J. Intellect. Prop. Manag.* **2008**, *2*, 411. [CrossRef]
62. Bertino, E. Trusted Identities in Cyberspace. *IEEE Internet Comput.* **2012**, *16*, 3–6. [CrossRef]
63. Linn, A.; Boyle, J.; McVey, M.; McKerlie, R.; Noble-Jones, R.; Dowell, F.; McLeod, G.; Copsey, D.; Murray, J.-A. *Digital Identity: Understanding How Students View their Digital Identity Working in Partnership with Students to Develop a Positive Digital Identity*; Enlighten Publications: Glasgow, UK, 2017.
64. Clarke, R. The digital persona and its application to data surveillance. *Inf. Soc.* **1994**, *10*, 77–92. [CrossRef]
65. Roussos, G.; Peterson, D.; Patel, U. Mobile identity management: An enacted view. *Int. J. Electron. Commer.* **2003**, *8*, 81–100. [CrossRef]
66. Crompton, M. *Proof of ID Required? Getting Identity Management Right*; Australian IT Security Forum, 2004; Available online: https://www.vs.inf.ethz.ch/edu/SS2005/DS/papers/identity/crompton_proof_of_id.pdf (accessed on 20 August 2020).
67. Heyman, R.; De Wolf, R.; Pierson, J. Evaluating social media privacy settings for personal and advertising purposes. *Info* **2014**, *16*, 18–32. [CrossRef]
68. Cameron, K. The laws of identity. *Microsoft Corp* **2005**, *12*, 8–11.
69. Rahaman, A.; Sasse, M.A. A framework for the lived experience of identity. *Identit. Inf. Soc.* **2010**, *3*, 605–638. [CrossRef]
70. Chatzakou, D.; Soler-Company, J.; Tsikrika, T.; Wanner, L.; Vrochidis, S.; Kompatsiaris, I. User Identity Linkage in Social Media Using Linguistic and Social Interaction Features. In Proceedings of the 12th ACM Conference on Web Science; Association for Computing Machinery (ACM): Southampton, UK, 2020; pp. 295–304.
71. Weeks, B.E.; Lane, D.S.; Kim, D.H.; Lee, S.S.; Kwak, N. Incidental Exposure, Selective Exposure, and Political Information Sharing: Integrating Online Exposure Patterns and Expression on Social Media. *J. Comput. Commun.* **2017**, *22*, 363–379. [CrossRef]
72. Goffman, E. *The Presentation of Self in Everyday Life*; Penguin: London, UK, 1959.
73. Culnan, M.J.; Armstrong, P.K. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organ. Sci.* **1999**, *10*, 104–115. [CrossRef]
74. Stewart, K.A.; Segars, A.H. An Empirical Examination of the Concern for Information Privacy Instrument. *Inf. Syst. Res.* **2002**, *13*, 36–49. [CrossRef]
75. Hurwitz, J.B. User choice, privacy sensitivity, and acceptance of personal information collection. In *European Data Protection: Coming of Age*; Springer: Geneva, Switzerland, 2013; pp. 295–312.
76. Xu, H.; Dinev, T.; Smith, H.J.; Hart, P. Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS Proc.* **2008**, *6*. Available online: https://aisel.aisnet.org/icis2008/6 (accessed on 20 August 2020).
77. Wentzel, K.R.; Wigfield, A. Academic and Social Motivational Influences on Students' Academic Performance. *Educ. Psychol. Rev.* **1998**, *10*, 155–175. [CrossRef]
78. Deci, E.L.; Ryan, R.M. Overview of self-determination theory: An organismic dialectical perspective. In *Handbook of Self-Determination Research*; Ryan, R.M., Ed.; University Rochester Press: Rochester, NY, USA, 2002; pp. 3–33.
79. Liu, Y.; Liu, R.-D.; Ding, Y.; Wang, J.; Zhen, R.; Xu, L. How Online Basic Psychological Need Satisfaction Influences Self-Disclosure Online among Chinese Adolescents: Moderated Mediation Effect of Exhibitionism and Narcissism. *Front. Psychol.* **2016**, *7*, 1279. [CrossRef] [PubMed]
80. Shen, C.-X.; Liu, R.-D.; Wang, D. Why are children attracted to the Internet? The role of need satisfaction perceived online and perceived in daily real life. *Comput. Hum. Behav.* **2013**, *29*, 185–192. [CrossRef]
81. Legault, L. Self-determination theory. In *Encyclopedia of Personality and Individual Differences*; Zeigler-Hill, V., Shackelford, T., Eds.; Springer: Cham, Switzerland, 2017; pp. 1–9. [CrossRef]
82. Ryan, R.M.; Deci, E.L. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *Am. Psychol.* **2000**, *55*, 68. [CrossRef]
83. Çelik, N.D.; Keklik, I. Personality Factors and Meaning in Life: The Mediating Role of Competence, Relatedness and Autonomy. *J. Happiness Stud.* **2018**, *20*, 995–1013. [CrossRef]
84. McKnight, D.H.; Choudhury, V.; Kacmar, C. Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Inf. Syst. Res.* **2002**, *13*, 334–359. [CrossRef]
85. Bartsch, M.; Dienlin, T. Control your Facebook: An analysis of online privacy literacy. *Comput. Hum. Behav.* **2016**, *56*, 147–154. [CrossRef]

86. Vansteenkiste, M.; Timmermans, T.; Lens, W.; Soenens, B.; Van den Broeck, A. Does extrinsic goal framing enhance extrinsic goal-oriented individuals' learning and performance? An experimental test of the match perspective versus self-determination theory. *J. Educ. Psychol.* **2008**, *100*, 387–397. [CrossRef]
87. Martela, F.; Ryan, R.M.; Steger, M.F. Meaningfulness as Satisfaction of Autonomy, Competence, Relatedness, and Beneficence: Comparing the Four Satisfactions and Positive Affect as Predictors of Meaning in Life. *J. Happiness Stud.* **2017**, *19*, 1261–1282. [CrossRef]
88. Weinstein, N.; Ryan, R.M.; Deci, E.L. Motivation, meaning and wellness: A self-determination perspective on the creation and internalization of personal meanings and life goals. In *The Human Quest for Meaning: Theories, Research, and Applications*; Wong, P.T.P., Ed.; Taylor & Francis Group: New York, NY, USA, 2012; pp. 81–106.
89. Hoffmann, C.P.; Lutz, C.; Ranzini, G. Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychol. J. Psychosoc. Res. Cyberspace* **2016**, *10*. [CrossRef]
90. Adjei, J.K. Explaining the role of trust in cloud computing services. *Info* **2015**, *17*, 54–67. [CrossRef]
91. Creswell, J.W.; Clark, V.L.P. *Designing and Conducting Mixed Methods Research*; Sage Publications: New York, NY, USA, 2007, 2017.
92. Demir, S.B.; Pismek, N. A Convergent Parallel Mixed-Methods Study of Controversial Issues in Social Studies Classes: A Clash of Ideologies. *Educ. Sci. Theory Pract.* **2018**, *18*, 119–149.
93. Behrendt, S.; Richter, A.; Trier, M. Mixed methods analysis of enterprise social networks. *Comput. Netw.* **2014**, *75*, 560–577. [CrossRef]
94. Venkatesh, V.; Brown, S.A.; Bala, H. Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *Mis, Q.* **2013**, *37*, 21–54. [CrossRef]
95. Latham, G.P.; Pinder, C.C. Work motivation theory and research at the dawn of the twenty-first century. *Annu. Rev. Psychol.* **2005**, *56*, 485–516. [CrossRef]
96. Vansteenkiste, M.; Ryan, R.M. On psychological growth and vulnerability: Basic psychological need satisfaction and need frustration as a unifying principle. *J. Psychother. Integr.* **2013**, *23*, 263. [CrossRef]
97. Mouakket, S.; Sun, Y. Examining factors that influence information disclosure on social network sites from the perspective of network externalities. *Ind. Manag. Data Syst.* **2019**, *119*, 774–791. [CrossRef]