future internet

MDPI

Article

Determining the Role of Social Identity Attributes to the Protection of Users' Privacy in Social Media

Katerina Vgena [1], Angeliki Kitsiou [1], Christos Kalloniatis [1,*] and Stefanos Gritzalis [2]

[1] Privacy Engineering and Social Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, GR 81100 Lesvos, Greece
[2] Department of Digital Systems, University of Piraeus, GR 18534 Piraeus, Greece
* Correspondence: chkallon@aegean.gr

Abstract: Drawing on digital identity theories, social software engineering theory (SSE), and the Privacy Safeguard (PriS) methodology, we examined the way that personal information uploaded on social media (SM) imposes privacy issues. Throughout a review on users' self-representation on SM, we examined the impact of self-determination and self-disclosure on users' privacy, and we identified the social attributes (SA) that cause privacy implications. This paper specifies 18 SA that users employ to achieve their optimal level of representation while summarizing possible ways that these attributes provoke users' identification. In particular, our research has shown that SM users represent their personas by unveiling SA to construct popular, representative, and conversational profiles. As disclosing SA increases privacy implications, we intend to help users build profiles that respect their privacy. Examining users' SA deepens our understanding of disclosing personal information on SM while leading to a better quantification of identity attributes; furthermore, users' top five most revealing attributes were summarized. Considering that SSE addresses users' privacy implications from an early stage of systems designing, our research, identifying the SA, will be helpful in addressing privacy from a socio-technical aspect, aiming at bridging the socio-technical gap by drawing designers' attention to users' social aspects.

Keywords: social media; socio-technical theory; identity; privacy

check for updates

Citation: Vgena, K.; Kitsiou, A.; Kalloniatis, C.; Gritzalis, S. Determining the Role of Social Identity Attributes to the Protection of Users' Privacy in Social Media. *Future Internet* **2022**, *14*, 249. https://doi.org/10.3390/fi14090249

Academic Editors: Francesco Buccafurri and Paolo Bellavista

Received: 11 July 2022
Accepted: 20 August 2022
Published: 24 August 2022

1. Introduction

The cloud helps users around the world store and access their content online. Despite the obvious benefits, using cloud services also points towards a better understanding of the reciprocal relationships between its main components, namely human and social aspects, and IoT (Internet of Things), as privacy and security issues were put under meticulous analysis due to the huge amount of data stored. As social cloud systems enable numerous organizations to offer services through social media networks because of the benefits provided by several functions, such as authentication [1], social cloud computing, or peer-to-peer social cloud computing, which use cloud services in ways that enable verification through a reputation system or a social network [2]. Therefore, social media represent a core part of cloud computing as they employ Internet of Cloud services while being utilized by users whose online behavior is tuned by their social attributes.

New privacy implications on social media (SM) arise [3] because SM combine technical characteristics (users' engagement in the online realm), while they interplay with disclosing and protecting users' SA. Users' SA should remain available on users' accounts to warranty proper social communications, while the amount and type of personal information should be examined from a privacy preservation spectrum [4].

Privacy is perceived as a "multifaceted concept" [5] (p. 1), including social aspects. Therefore, an interdisciplinary approach is needed, considering psychological, social, and cultural aspects [6]. Due to these aspects, software designers face challenges to protect users' privacy to determine when, how, and what information is disclosed on SM.

Social aspects are considered an integral part when designing privacy-aware information systems in social software engineering (SSE). Thus, the main principles of SSE are essential for setting the principles for protecting users' privacy from an early stage of the system's designing [7,8]. Various implications may be addressed in the early stages, i.e., adjusting and implementing socially aware privacy requirements to handle users' privacy in an interdisciplinary manner. This principle is compatible with the principles of the EU Regulation (GDPR), which roughly describes two privacy principles: privacy by design (incorporate privacy requirements from an early stage of system designing) and privacy by default (impose strict privacy regulations to a system by default rather than more lenient ones).

Researchers should focus on identifying the social aspects that can target users' identities when disclosed on SM to properly assist developers when designing privacy-aware information systems. Networking platforms have drawn users' and researchers' attention on the basis of implications and patterns to deal with information disclosure [9]. This paper intends to examine privacy issues in relation to users' SA [8,10], as they provide information about user's identification [4] with potentially harmful effects for the user [3].

This paper investigates the SA, which through the processes of self-determination and self-disclosure can lead to users' identification. We focus on the way that self-determination and self-disclosure function while users represent themselves in the online sphere, and the way that users' representation may impose privacy implications because of identification or targeting issues. Bridging the socio-technical gap between social attribute disclosure and privacy requirements requires a detailed quantification of the respective SA to design privacy-aware information systems. The list of the eighteen attributes shall point towards this direction. Our research is based on the principles of SSE, focusing on the social aspects of computer engineering, in the field of non-functional requirements. The domain of our research is social media networks, as we draw on SM for all the examples of the paper.

More specifically, after the introduction, there is a short analysis of digital identity and possible privacy implications on SM. Section 3 discusses the role of self-determination and self-disclosure on the representation of users' personas online. Section 4 reviews users' SA, drawing on previous bibliography. Section 5 presents the relationship among social domains, attributes, and variables in the process of user identification. The last section concludes the paper while making final remarks.

2. Digital Identity and Privacy Implications on Social Media

2.1. Digital Identity and Social Aspects

Digital identity's definition is one of the most intriguing definitions in social sciences [11–14]. SI became even more interesting, since identity was filtered through the internet layer to become digital or online identity [15,16]. Different notions have merged together, as digital representations tend to resemble the very true self of each user [15,17].

Traditional space and time have merged, creating digital stages (combinations of place and time) via continuously logged-into web devices [13,18]. Understanding SI through its main characteristics, namely complexity, multiplicity, permeability, and overlapping [19,20], can be seen as Anthony Giddens underscored, as a "project": as an ongoing, endless process of the construction of an individual's persona [19] due to environmental and societal influences [13].

The deconstructive theory and poststructuralist notions of bricolage are also part of users' activities and performances online [15]. This is the rationale that we are borrowing and implementing in our paper when talking about users' Faces and the way that users employ different Faces to perform under distinct social circumstances (Frame, Time, Stage) when complying with the respective social norms implied by the context [21,22]. Social norms are important notions of the states of privacy [23] because they are parallel to the notion of the reserve (the practice of mental distancing from close relationships when needed). Tracking social norms may provoke identification when regenerated to track user's online patterns and expected ways of behavior by third parties [24,25].

Different Faces or expected ways of behavior should be disclosed by the users themselves as they are expected by other users. "Faces are a kind of social user's manual" [26] (p. 18) which enable human interaction. Alternative or synonymous versions for signifying the representation of the user's Face can be "Identities", "Selves", or "Versions". These variations of the individual, as different realizations of his or her persona, function in unique "timeframes", meaning specific time-spaces or periods of time [13,19,26]. Minor differentiations in time might imply additional space variations, which intensify the necessity for adopting different "Faces" to function properly in specific contexts (conventional or digital) or around the clock.

Identity management, on the other hand, discusses what should remain hidden on behalf of the users. In this regard, several systems, anonymization techniques, and privacy-enhancing technologies have been developed and multiplied for managing identity, access control, and ensuring privacy [27–29] such as OpenID, PKI, SAML, Virtual Private Networks, DNS Security Extension, and Private Information Retrieval. These would typically support users' de-identification; thus, a universal identity management standard is not yet embraced [28]. Developers usually design and deploy centralized systems that enable users' information linkability among devices and services, risking their identification [30]. This occurs because identity management is addressed as a technical issue concerning only users' verification, authorization, and roles within the systems and services. However, identity within the cloud is a broader notion, including many types of information and representations of a user such as legal and digital representations and attributes inferred from usage or behavioral data [28] and, therefore, cannot be addressed from a technical view only. Considering this, it is the notion of Face, drawn from SI Theory, which determines users' behaviors and representation, leading to users' disclosed attributes, while identity management imposes what kind of information should remain hidden under a technical aspect. For example, gender through the LGBDQ+ community is analyzed in how university students employ social media applications for identity management. Social factors manifest the way the students express the multiplicity of their identities as far as self-censorship is concerned [31]. Another important aspect in addition to gender is the way young people manage their online and offline privacy concerns, formulating proper privacy education and identity management [32]. Online and offline are considered continuous in the sense that sharing friends and using mobile devices blurs the limits between the two [32]. As authors argue in [33], combining users' information can lower users' trust, leading to suppressing personal identity attributes on behalf of the user; researchers propose that users' control on identity management will be of benefit. The use of digital identity signifies users' attempts to represent themselves with valid identity information to communicate with other "real" users while online [13,34]. Using enormous amounts of information creates a lenient stance towards disclosing their real identity. Real identity as a synonym to digital identity has also been discussed by previous research [34,35], signifying that there is no difference between the real, offline, and online social representations of the user. Performing as postmodern online subjects, we draw on Marwick's point on the deconstruction of the "online" and "offline identity" binary in our everyday practice. Her main arguments lie in showing that users log in to SM both in "real-life contexts" and ubiquitously via wireless portable devices [13].

Digital identities are conversational ones, or as Papacharissi (2012) has defined them, "networked selves", which facilitate communication by blurring private and public lives [36], while turning part of users' privacy into entertainment content to be consumed as "extimacy" for entertainment purposes [20,24]. Hinton and Hjort's "intimacy online" is users' need to project everyday moments to construct their online identity [18]. Despite users' tendency to build realistic representations of their identity, there is a tendency towards an idealized representation of themselves through selecting content in reference to their context or audience [34].

Rodota stresses that "In the past identity was defined by the words 'I am what I say I am', but today 'I am what Google says I am'" [37]. Online privacy has acquired a new meaning, as it is “one of the major concerns when publishing or sharing social network data” [38] (p. 1). Identity is perceived as a social “product”, which is supposed to be “shaped” and “shared” by the users themselves along with what their friends’ network narrates about them [36,39].

2.2. Privacy Implications and the Privacy Paradox

The repetitive posting trend of photographs on SM drew researchers’ attention due to the huge amount of personal and/or sensitive information revealed [34]. Users’ persistent engagement on SM tends to cultivate “more lenient privacy attitudes and beliefs” [40] (p. 4). “Users’ dilemma”, [34] or the privacy paradox, as it is widely known [16,41,42], should be considered as users waffle between their privacy concerns and their need to build popular, representative, and conversational profiles [16,34,43–48].

Photographs unveil details about “babyfaces, credit cards, phone numbers, social security cards, house keys and other personally identifiable information” [3] (p. 1) which will not be removed even after deleting the content [3,49,50] or the account. Implications related to photographs are referred to as “visual privacy leaks” and may harm users’ financial or personal lives. Sharing the same content across SM can facilitate users’ identification [3,13].

Marwick’s “context collapse” raises privacy implications by discussing the revelation of users’ content to unwanted audiences [51]. This revelation hints at social surveillance and surveillance technologies, as far as online social habits of networking are concerned [52]. Bigger audiences than originally intended, or false presuppositions of one’s online audience, may lead to self-disclosing to unwanted social groups [15,16,53]. “Today, almost everyone’s digital profile is looked at by employers, banks, family, friends and future significant others, educators, and hackers” [54], imposing implications regarding social surveillance through “context” or “time collapse”. Marwick’s notion of “time collapse” [55–59] signifies the consistent omnipresence of digital traces of users’ identity through time. As stated in J. D. Lasica’s remark, “our pasts are becoming etched like a tattoo into our digital skins” [55] (p. 2). Time collapse is readopted by Raynes Goldie, who underlines that “Facebook makes things that should just have happened in passing totally permanent and public” [60] (p. 11).

Privacy is “a prerequisite for being included in the participation society” [17]. It should be warrantied as an individual right and a public good in our digital society to ensure freedom of speech in the electronic sphere [11]. Privacy and freedom are closely associated with the European perception of the “right to be left alone”, one of the fundamental rights and freedoms protected by the right of data protection in the Charter of Fundamental Rights of the EU [17].

Focusing on the role of self-determination and self-disclosure as users’ unveiling mechanisms on SM can help researchers examine users’ representations while managing privacy implications online.

3. The Role of Self-Determination and Self-Disclosure in Users’ Privacy

3.1. Privacy and Self-Determination

One of the most intriguing approaches on self-determination was provided by Westin long before the era of SM. In his work, he prophetically described the challenging future of the USA in regard to privacy issues [61]: the astonishingly high number of self-revelations in which many on the internet engage, especially among the young generation, point towards a “let it all hang out” philosophy” [61] (p. 20). This extract can also describe today’s reality in most parts of the Western world, irrespective of the country of origin, because of the similarities among the sociopolitical systems of the Western world [6]. Debatin defines self-determination in privacy as a “moral principle and right” that enables users to control their disclosures; it is “a basic positive moral and legal principle of privacy protection” [62] (p. 51).

Users tend to blur the notions of self-determination and authenticity. Authenticity has been analyzed as an equivalent to self-determination and an expression of the so-called “true-self” or “core-self” [62]. It is defined as “the unobstructed operation of one’s true-

or core-self in one's daily enterprise" [62] (p. 73). Extending self-determination to signify authenticity in one's public profile further supports the deconstruction of the privacy paradox from a psychological point of view. Authenticity is also seen as the main reason for users to disclose their real name [15] along with the reason for the success of some of the most prevailing networking sites today. The installation of location-based services in mobile devices has made real-time updating of profiles and "instaposting" a way of life for young people, especially for a generation that has made use of these applications long before their adulthood, to exchange information between pairs of people, groups, or among individuals and organizations [12].

Westin's multifaceted definition describes four states of privacy, namely solitude, intimacy, anonymity, and reserve [6,23]. This is one's need for privacy and may be read as the "balance between a desire for disclosure and social participation and a desire for withdrawal into one of the ′states′ of privacy" [23] (p. 1). When the balance is optimized, a user may experience the optimal level of privacy between his or her social exchanges, self-disclosure, and the right to be left alone [16]. Privacy is dynamic (adaptive notion) and non-monotonic (different levels of granularity) [6]. Individual privacy (states of privacy) refers to the constantly changing nature of users' needs [61]. Users tend to function in the entire spectrum, alternating from the right to be left alone to posting personal information constantly [16].

Self-determination and privacy warranty the protection of users' Faces from content collapse [62]. This definition supports our claim that changing contexts require the presence of different social roles, Faces, in different stages (place and time). The notion of Face is drawn from sociology theories and was used in the previous section to signify the expected way in which an individual should normally function in each context. For example, when an individual is present at work, they are expected to carry on in their encounters while wearing the Face of the employee.

3.2. Privacy and Self-Disclosure

Self-disclosing parts of users' identities impose additional privacy implications to the ones already in place due to potential online threats. Self-disclosure is the practice of intentionally unveiling personal information about one's identity to another person or an audience; therefore, it is directly related to privacy [62]. A user's true-self is revealed through self-disclosure: the process that makes the self of one user known to others through any online message [16]. Self-disclosure could be perceived as a contradicting notion to privacy, given that it reveals users' personal information as if they are in a constant battle between what users want to reveal and what they want to conceal [16,53,62].

Self-disclosure is necessary to guarantee successful interactions as a tool for ″selective control of access to the self" [16] (p. 2), determining what is visible to whom and when. It is a prerequisite for establishing social relationships and a necessary step towards building trust and creating social proximity among individuals [12].

Despite users' needs for representation, managing their privacy is also important. Users' management and setting of boundaries are some of their options for limiting one's access. However, even when measures are taken, the content will be available to the user's "Friends" eternally, raising long-term consequences. SM Friends blur the notion of proximity between people, as they signify a wide range of social relationships, from relatives and close friends to colleagues and acquaintances. This vagueness fluctuates the number of Friends from a few to many hundreds [53,62]. Thus, users may be unaware of their actual self-disclosure on SM because of spontaneous or unconscious communication with their close friends which can easily be susceptible to third parties.

Setting boundaries and managing one's self-disclosure options can represent users' needs in establishing different types of relationships and control of the repercussions of context and time collapse. As privacy is a dynamic process that requires constant adjustments depending on users' changing needs, managing one's self-disclosure options may prove valuable when handling privacy implications. Privacy is not "as a process of retreat", but an effort to accomplish "different degrees of self-disclosure in different situations" [62] (p. 150).

Uncontrollable self-disclosure, unmediated social interactions, and unstoppable sharing of identity traits have been included in the term "digital crowding", which triggers potential threats [62]. Apart from the inherent danger when someone discloses too much information about oneself, drawing on the principles of SI Theory, we add the dangers related to the overlapping of social spheres and users' inability to wear the right Face in the right Stage [21]. Audience diversity can perplex users when handling opposing audiences at the same time [53].

Self-determination and self-disclosure are two distinct notions, yet they can be strongly interrelated. Self-disclosure is presupposed as a means for transmitting users' private information, controlling who will be allowed in and what type of information will be accessible. Self-determination or self-representation refers to the way this information will be handled and consumed.

Having discussed two crucial notions of digital identity and their implications when managing users' personas, we draw on previous research to proceed in labeling the social aspects which could be beneficial in quantifying the social parameter in the domain of SM.

4. Revealing Social Attributes: A Review

To protect users' privacy when designing privacy-aware information systems, we should explore users' SA. Users disclose different characteristics and layers of granularity because of their different perceptions of privacy. Accordingly, researchers often refer to personalized privacy requirements to address this need [63]. To determine users' SA on SM, we conducted a review to list the SA that, to the best of our knowledge, users disclose while posting online. These attributes provide the necessary background for designing measuring scales appropriate for examining users' digital identities.

We have screened a total number of 1,724,450 papers in our review. Keywords, such as digital identity, social media, social attributes, users' self-representation, and users' identification, were extracted from Google Scholar, Scopus, IEEE, ScienceDirect, and Semantic Scholar from 2001 to 2021. The aim of this study was to identify articles that examine users' concerns, users' privacy risks, or strategies from a socially oriented approach to ensure that we extracted SA that were not necessarily in previous research regarding social and location attributes, drawing on the Privacy Safeguard (PriS) methodology [5]. Location was added as an integral part of users' representation on SM. Researchers included only articles which combined social identity, location, and privacy theories on social media in order to include only papers which matched the interdisciplinary approach of the study. Table 1 presents the criteria applied during the exclusion process.

Table 1. Exclusion Criteria.

Exclusion Criteria
1. Studies discussing users' characteristics using social theories exclusively
2. Studies discussing users' characteristics using location theories exclusively
3. Studies discussing users' characteristics using privacy theories exclusively
4. Studies combining socio-location characteristics without privacy concepts
5. Studies combining privacy concepts and social characteristics without location theories on social media
6. Studies not proposing possible solutions for quantifying the relevant information for future research
7. Studies not accessible in full text
8. Studies not written in English

More precisely, the aim in this paper was to examine users' social attributes, drawing on social and privacy concepts in a way that could lead to possible quantifications of the above-mentioned characteristics pointing towards a possible extension via the creation of a proper tool (questionnaire, interviews) as a future step to investigate users' practices on social media. Guidelines and research recommendations based on the conceptual model of the Prisma 2020 flow diagram are incorporated in the reviewing process [64]. A Prisma 2020 flow diagram is used to visually represent the reviewing process of our paper. Figure 1 represents an adjustment of the proposed visualization of this process:

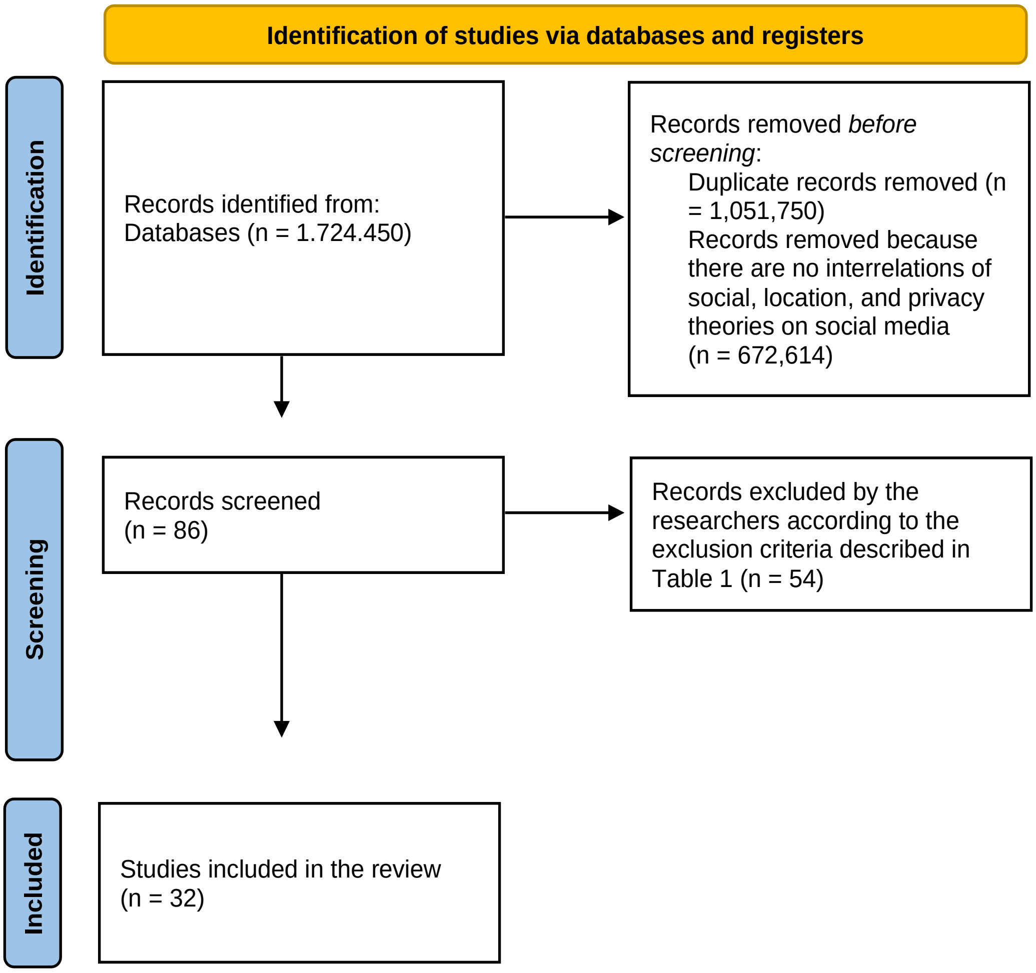
Identification of studies via databases and registers
Identification
Records identified from:
Databases (n = 1.724.450)
Records removed *before screening*:
Duplicate records removed (n = 1,051,750)
Records removed because there are no interrelations of social, location, and privacy theories on social media
(n = 672,614)
Screening
Records screened
(n = 86)
Records excluded by the researchers according to the exclusion criteria described in Table 1 (n = 54)
Included
Studies included in the review
(n = 32)

Figure 1. Methodology processes: Prisma 2020 flow diagram.

After the initial search, many articles had to be excluded as interrelations among the notions of social, location, and privacy concepts could not be detected. After extracting an initial list of SA, further socio-cultural attributes were added. Duplicates, studies not accessible in full text, and non-English articles were excluded. A total of 32 papers were reviewed, extracting 18 SA. Each attribute is presented in Figure 2 alongside the reviewed papers that refer to the respective attribute of SI:

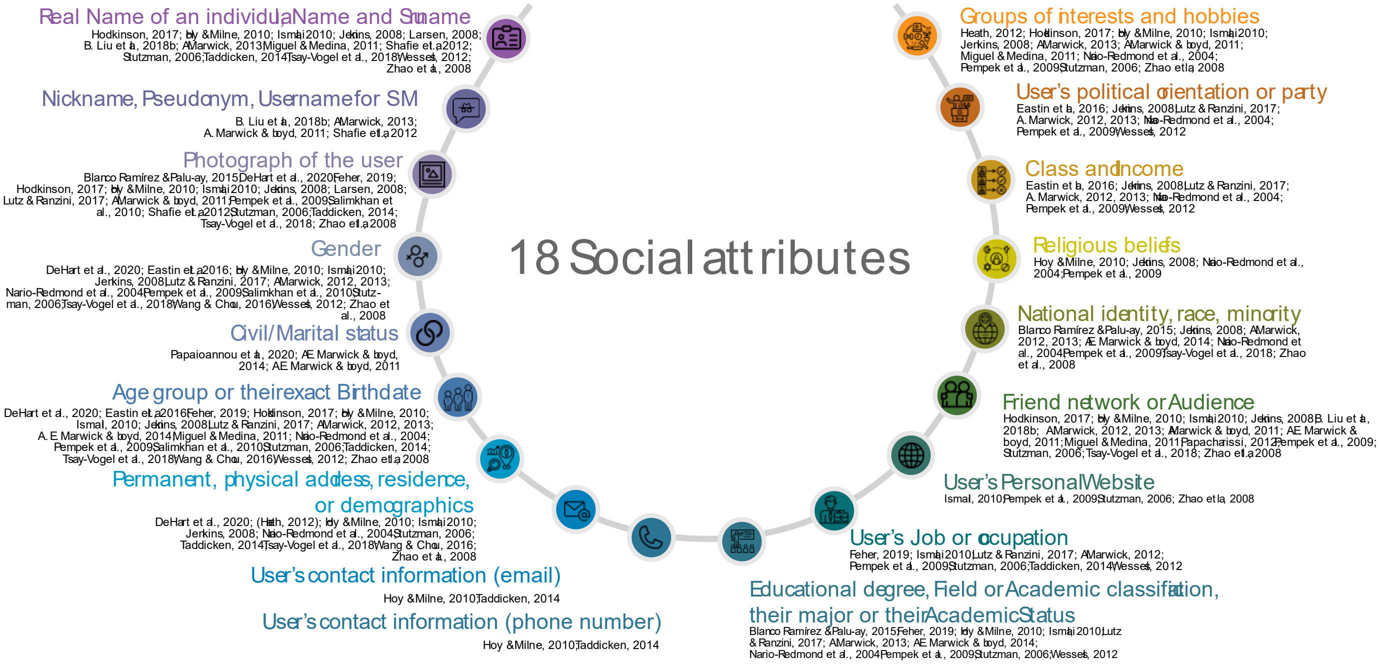
18 Social attributes
Real Name of an individual, Name and Surname
Hodkinson, 2017; Hoy & Milne, 2010; Ismail, 2010; Jenkins, 2008; Larsen, 2008; B. Liu et al., 2018b; A. Marwick, 2013; Miguel & Medina, 2011; Shafie et al., 2012; Stutzman, 2006; Taddicken, 2014; Tsay-Vogel et al., 2018; Wessels, 2012; Zhao et al., 2008
Nickname, Pseudonym, Username for SM
B. Liu et al., 2018b; A. Marwick, 2013; A. Marwick & boyd, 2011; Shafie et al., 2012
Photograph of the user
Blanco Ramírez & Palu-ay, 2015; DeHart et al., 2020; Feher, 2019; Hodkinson, 2017; Hoy & Milne, 2010; Ismail, 2010; Jenkins, 2008; Larsen, 2008; Lutz & Ranzini, 2017; A. Marwick & boyd, 2011; Pempek et al., 2009; Salimkhan et al., 2010; Shafie et al., 2012; Stutzman, 2006; Taddicken, 2014; Tsay-Vogel et al., 2018; Zhao et al., 2008
Gender
DeHart et al., 2020; Eastin et al., 2016; Hoy & Milne, 2010; Ismail, 2010; Jerkins, 2008; Lutz & Ranzini, 2017; A. Marwick, 2012, 2013; Nario-Redmond et al., 2004; Pempek et al., 2009; Salimkhan et al., 2010; Stutzman, 2006; Tsay-Vogel et al., 2018; Wang & Chou, 2016; Wessels, 2012; Zhao et al., 2008
Civil/Marital status
Papaioannou et al., 2020; A.E. Marwick & boyd, 2014; A.E. Marwick & boyd, 2011
Age group or their exact Birthdate
DeHart et al., 2020; Eastin et al., 2016; Feher, 2019; Hodkinson, 2017; Hoy & Milne, 2010; Ismail, 2010; Jenkins, 2008; Lutz & Ranzini, 2017; A. Marwick, 2012, 2013; A. E. Marwick & boyd, 2014; Miguel & Medina, 2011; Nario-Redmond et al., 2004; Pempek et al., 2009; Salimkhan et al., 2010; Stutzman, 2006; Taddicken, 2014; Tsay-Vogel et al., 2018; Wang & Chou, 2016; Wessels, 2012; Zhao et al., 2008
Permanent, physical address, residence, or demographics
DeHart et al., 2020; (Heath, 2012); Hoy & Milne, 2010; Ismail, 2010; Jerkins, 2008; Nario-Redmond et al., 2004; Stutzman, 2006; Taddicken, 2014; Tsay-Vogel et al., 2018; Wang & Chou, 2016; Zhao et al., 2008
User's contact information (email)
Hoy & Milne, 2010; Taddicken, 2014
User's contact information (phone number)
Hoy & Milne, 2010; Taddicken, 2014
Groups of interests and hobbies
Heath, 2012; Hodkinson, 2017; Hoy & Milne, 2010; Ismail, 2010; Jerkins, 2008; A. Marwick, 2013; A. Marwick & boyd, 2011; Miguel & Medina, 2011; Nario-Redmond et al., 2004; Pempek et al., 2009; Stutzman, 2006; Zhao et al., 2008
User's political orientation or party
Eastin et al., 2016; Jenkins, 2008; Lutz & Ranzini, 2017; A. Marwick, 2012, 2013; Nario-Redmond et al., 2004; Pempek et al., 2009; Wessels, 2012
Class and Income
Eastin et al., 2016; Jenkins, 2008; Lutz & Ranzini, 2017; A. Marwick, 2012, 2013; Nario-Redmond et al., 2004; Pempek et al., 2009; Wessels, 2012
Religious beliefs
Hoy & Milne, 2010; Jenkins, 2008; Nario-Redmond et al., 2004; Pempek et al., 2009
National identity, race, minority
Blanco Ramírez & Palu-ay, 2015; Jenkins, 2008; A. Marwick, 2012, 2013; A.E. Marwick & boyd, 2014; Nario-Redmond et al., 2004; Pempek et al., 2009; Tsay-Vogel et al., 2018; Zhao et al., 2008
Friend network or Audience
Hodkinson, 2017; Hoy & Milne, 2010; Ismail, 2010; Jenkins, 2008; B. Liu et al., 2018b; A. Marwick, 2012, 2013; A. Marwick & boyd, 2011; A.E. Marwick & boyd, 2011; Miguel & Medina, 2011; Papacharissi, 2012; Pempek et al., 2009; Stutzman, 2006; Tsay-Vogel et al., 2018; Zhao et al., 2008
User's Personal Website
Ismail, 2010; Pempek et al., 2009; Stutzman, 2006; Zhao et al., 2008
User's Job or occupation
Feher, 2019; Ismail, 2010; Lutz & Ranzini, 2017; A. Marwick, 2012; Pempek et al., 2009; Stutzman, 2006; Taddicken, 2014; Wessels, 2012
Educational degree, Field or Academic classification, their major or their Academic Status
Blanco Ramírez & Palu-ay, 2015; Feher, 2019; Hoy & Milne, 2010; Ismail, 2010; Lutz & Ranzini, 2017; A. Marwick, 2013; A.E. Marwick & boyd, 2014; Nario-Redmond et al., 2004; Pempek et al., 2009; Stutzman, 2006; Wessels, 2012

Figure 2. User's Social Attributes on Social Media.

Figure 3 illustrates all SA which can represent users' online personas on SM. These attributes can be uploaded to a different level of granularity or combined, depending on users' preferences.

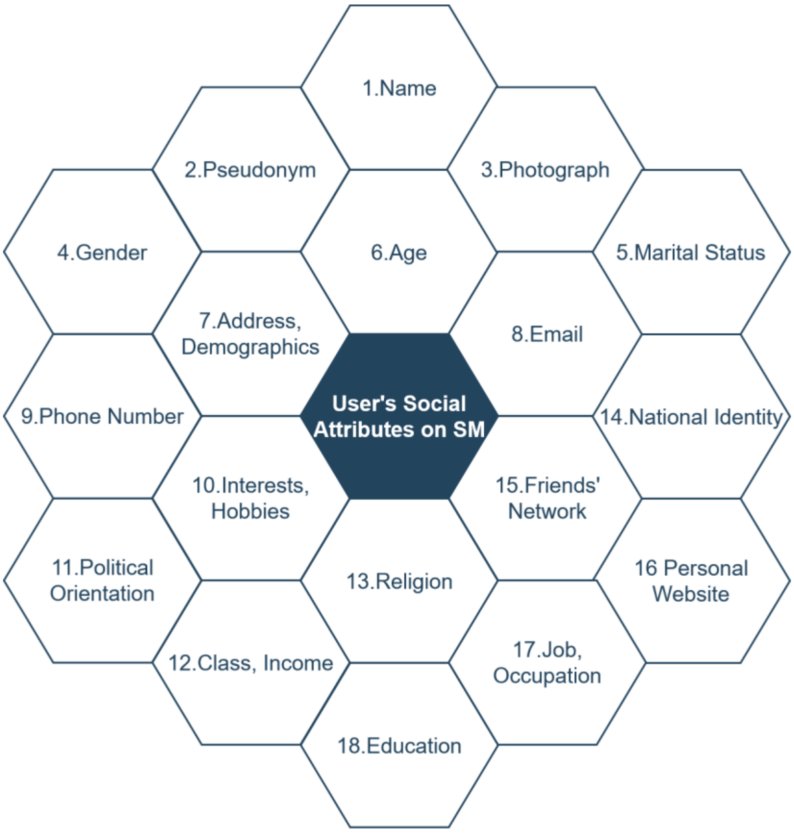

Figure 3. User's Social Attributes on Social Media.

Users tend to maintain profiles in different applications, such as Facebook, Twitter, and YouTube; sometimes, they choose to link them with other SM applications, such as Instagram, LinkedIn, Pinterest, Tumblr, MySpace, Grindr, Tinder, Snapchat, Flickr, or CouchSurfing [18,65], or with Skype, online shopping or banking, their eBay account, or potential online doctors' appointments [35]. Users establish connections among different SA of their digital identity as they update their profile information while posting and commenting online [40]. Linking users' profiles creates an ecosystem in which they maintain the same "username and basic information" to promote self-representation on SM [13].

Establishing connections triggers privacy implications due to users' identification through different platforms. Time is also significant, as underage students share personal information that shall remain available throughout their adulthood. Arguably, the average student will have already created a digital identity when entering college through information disclosure from Google, Apple, Amazon, Facebook, Instagram, Microsoft, and Twitter [54].

The shared information can include opinions, personal experiences, thoughts, feelings, fears, concerns, and knowledge, but more often than not, users' full names, contact information, and private photos are going to be "digitally stored and therefore persistent, replicable, scalable and searchable as well as shareable" [16] (p. 1). Possible threats imposed by the amount of personal information can be filtered through users' prior mobile experience and awareness of the content of their posts [66].

Having completed the review on identity attributes, we will proceed in discussing our findings and establishing relationships among general domains, attributes, and variables of users' digital identities.

5. Discussion

5.1. Domains, Attributes, and Variables

After listing the 18 SA that, to the best of our knowledge, users share to represent themselves, we investigated the ones which can disclose the SI principles according to SI Theory [4,10,19,26], already examined in our previous research, regarding the methodology of the categorization of the social domains. The notions of Face, Frame, Stage, Time, and Activity or Performance were introduced and explained in [21,67]; in this paper, they are linked to the notions of social determination and disclosure to draw the interrelations among social domains, attributes, and variables in a way that can benefit our understanding when designing privacy-aware systems.

SA are categorized based on the general domains of SI which function as umbrella terms. Face can be disclosed through a user's name or surname, nickname, profile picture, gender, age, address or place of residence, education, affiliation, or job. Additional attributes can be drawn from a user's personal website, friend network, national or religious identity, class or income, or groups of interests and hobbies. Disclosing a user's photograph, address, place of residence, contact information, affiliations, job, friend network, national identity, or groups of interests can prove descriptive of their place of presence too. Moreover, time can be disclosed via SA on SM through photographs, education, affiliations, jobs, users' websites, and groups of interests. Furthermore, the Stage represents the combination of Frame and Time, so it sums up the total of the aforementioned attributes. Nicknames, photographs, education, affiliations, jobs, users' personal websites, friend networks, national or religious identities, class, income, political orientation, or groups of interest and hobbies can reveal information about a user's Activity or Performance.

Table 2 combines the 5 general domains of SI and the 18 SA. Face discloses information on who users are, Frame is descriptive of Place, and Time refers to the attribute of when an action took place. Stage conveys information on both Place and Time, while Activity or Performance deals with information about what kind of actions the user performed.

Table 2. Social Identity Domains and Social Attributes on Social Media.

SI Domains	SA on SM
Face	1–6, 8–18
Frame	3, 7–11, 13–14, 17–18
Time	3, 10–11, 12, 18
Stage	3, 7–14, 18
Activity or Performance	2–3, 10–18

After the initial categorization, each of the SA on SM were examined, while possible explanations for disclosing attributes were discussed. Face can be disclosed through almost all SA. The most common practice for a user is to share his or her real name. Additionally, users may opt for a nickname as a SM username representation. In that case, even the fonts and pseudonyms of the users can represent parts of their identity to visualize representations of themselves while distinguishing themselves from others [13,34,39,46,47,60,68–70]. Nicknames can potentially reveal a user's Activity or Performance (MusicLover).

Discussing online naming devices, we should mention the long discussion of researchers between using real names or pseudonyms online. Users are keen on using their real names, as some of the world's leading networking sites are pointing towards this direction, such as Facebook, Google, and LinkedIn [15]. Although this trend was not common during the early days of the internet, it has become extremely popular. Sharing photographs is another common practice among SM users, who upload enormous amounts of information [18]. Sharing pictures and videos is estimated to increase continuously as technology and SM grow [3]. In particular, users tend to share a desirable image of themselves [71], so they upload photos with positive (idealized) depictions, without any negative images [18,48].

In extreme cases, such as the "catfish", users represent themselves in totally false identities for several reasons [18]. Alternatively, some users may opt for neutral depictions, such as pictures of flowers, landscapes, or cartoons, when choosing their profile picture [46]. Another famous practice is to share videos, which are much more descriptive than sharing photographs (a combination of image, motion, and sound) [40,45,72].

Photographs' power of representation is one of the major findings of Table 1, as all five attributes of SI can be communicated. Disclosed SA through photographs can trigger privacy implications which should be investigated, focusing on the social aspects of SSE.

Gender discloses information about the user's Face. It can also be revealed through one's relationship status and sexual identity or orientation [13,35,48,65,69,73–75]. For example, Tinder, a location-based real-time dating application, uses mobile media services for communicative purposes among people who are interested in meeting new potential partners [65]. However, combining gender and location can trigger neighborhood attacks. Neighborhood attacks signify the access of third parties to a user's friend account, and the susceptibility of the user to targeting, surveillance, or re-identification [14].

Users' Faces can be revealed through age groups or their exact birthdate. Except for direct unveiling, users reveal information about their age covertly, via school information (combined age and place of origin) [48,69,75]. Another common practice is to share their year of graduation [74].

Face, Frame, and Stage can be assumed by having access to users' demographics. These include addresses or permanent places of residence, hometowns [3,45,69,74,75], high schools [45], zip codes [69,75], countries [69,75] and regions [72,76].

Face, Frame, and Stage can be extracted by users' contact information, through Email addresses [10,48,69,74,75] or phone numbers [3,19,45,48,69,75]. The email address is more prone to disclose users' SA than a phone number, as it can contain real names, age, birthdate, workplace, or address if a professional email is used. Phone numbers may disclose geographical information through regional codes.

Education, affiliations, or a user's job are other important attributes for when users want to represent themselves on SM. These attributes represent the second most important finding in our paper, as they can disclose all five domains of SI. Institutional affiliations carry a plethora of implied conclusions about the user [18,35,48,60,74]. Status and role appear as "a collection of rights and duties" [19] (p. 164). According to this point of view, "husband", "professor", "employee", or "friend" are statuses, which carry certain roles, social norms, or behaviors [19,26]. A common practice among academics is to use SM applications to post about their research to engage researchers of similar subjects [18]. Users disclose Face, Stage, and Activity in one post. Educational background and occupation are susceptible to making mutual assumptions about the existing or future groups of interests of users' CVs, and they can be linked to marking social class or drawing inferences about their tastes [77].

Face, Time, Stage, and Activity or Performance can be drawn from disclosing personal websites. Disclosing personal websites can be linked to users' common practice of linking different SM platforms. Linking accounts provides advantages, such as better representation or easier access to platforms, yet it poses additional privacy implications due to probable identification by malicious attackers.

Friends' network and users' audiences are important for representing one's persona, as Face, Frame, Stage, and Activity or Performance might be disclosed. SM are social constructions and users' identities are powerful tools for reaching audiences and conducting social performances [39]. Friends' networks may carry geographical connotations as far as our close friends or the majority of our acquaintances are concerned. Users' connections can be quite informative while sometimes they can be used to state users' social capital [53,74]. Users share information about their social status or social role [76] to increase their social capital or manage the impressions of other users [24]. Users share location information about their presence at their university not only for disclosing their geographical position but also to gain prestige as members of the academia [73].

Sensitive information regarding national identity, race, or religious beliefs are presented on SM. National identity can unveil information about Face, Frame, Stage, and Activity or Performance. Combining Face, Frame, and Activity is powerful enough to target the user via disclosing religious beliefs. Religious representations, such as the burqa, can easily be identified on a profile by a photograph post [19]. Users may reveal information about their class, income, and political orientation or party through posting photographs, quotes, personal beliefs, or engaging in online commenting. Face, Frame, and Activity might be unveiled on both their and their friends' profiles.

Another important finding of the table above relates to the revelation of all five attributes of SI through groups of interests and hobbies. Users represent themselves by talking, posting, or sharing information about their interests. Pushing the like button or getting enrolled in groups and pages is another very common practice that users employ to become acquaintances with people with shared interests.

Traffic flows, mentions, likes, and consumer-oriented options and tendencies are descriptive of users' preferences, as well as the brands and services that they follow [78]. Group affiliation [69,75], favorite music [13,36,69,75], favorite videos [13], favorite films [13,36,45,74,75], favorite books [13,36,45,69,74,75], personal statements by famous people and narrative descriptions [48,69,75,79], favorite TV shows [69,75], and opinions, values, and ethics [40,60] are shared for the same reason.

The most revealing SA are illustrated in Figure 3. A double-check was conducted on which and how many of the SI general domains correspond to the SA to evaluate the aforementioned attributes on SM while putting them on an evaluative scale from the most to the least revealing.

According to Figure 4, the most revealing SA include all five general domains of SI, namely users' photographs, education, occupation, personal websites, and groups of interests. Additional privacy implications can be raised due to potential inferences when combining them. Revelations of one of them or of a combination of them lead to additional inferences, increasing users' identification while imposing privacy implications.

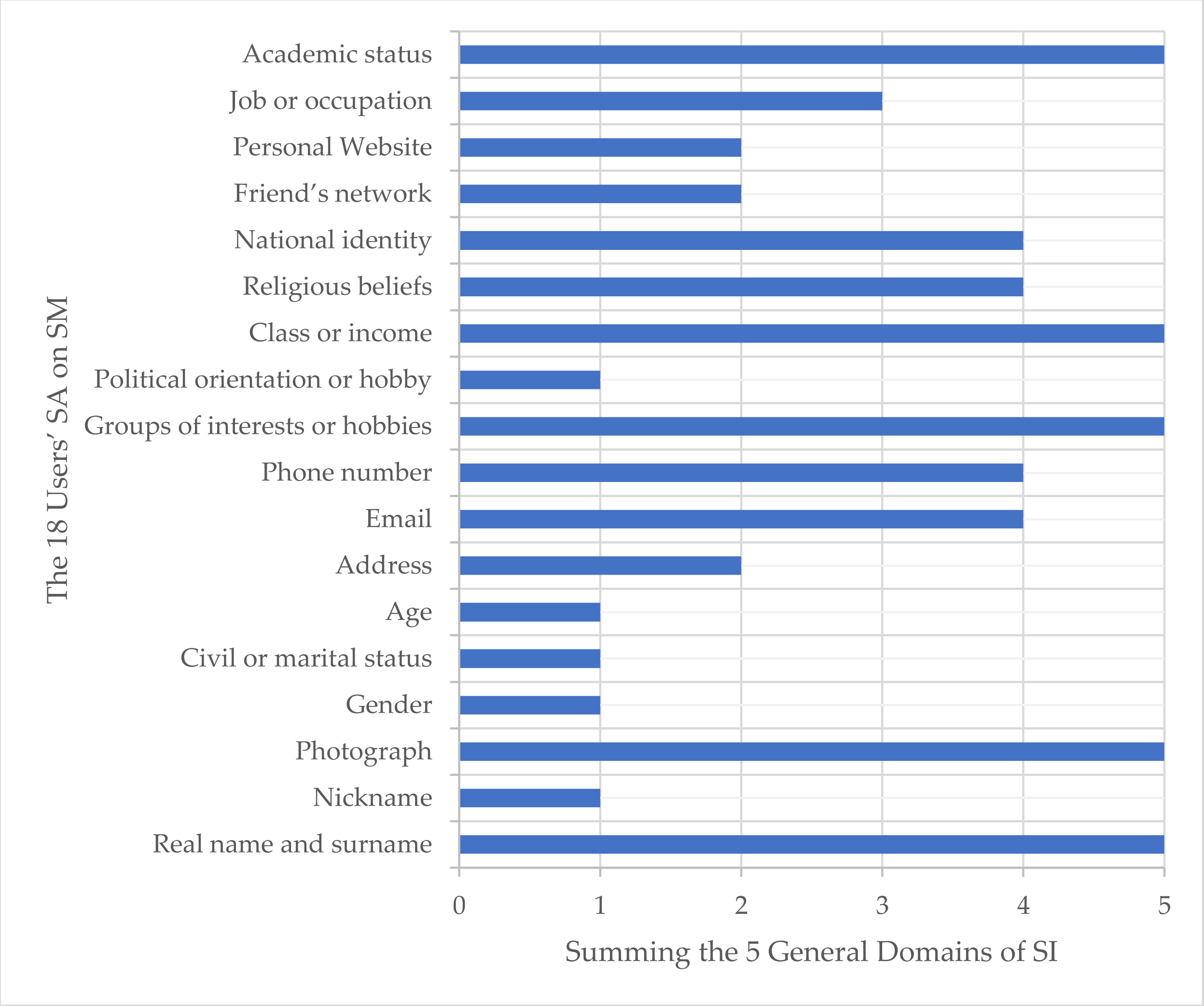

Figure 4. The Most Revealing Social Domains on Social Media.

Making inferences by linking different accounts, combining information revealed by different parties [38], or "accumulated SM posts, particularly when coupled with other data sources such as demographic data, statistical data or household data, which are increasingly available as open-source repositories" [80] (p. 2), intensifies the use of personal information as a ”commodity” [12] or as entertainment content [20]. Inferences about one's private information and, therefore, identity can be discussed in a more technical approach [38]: using structure anonymization methods to build upon users' privacy protection of combined data published by various parties.

In the subsequent section, we move to classifying the fundamental social domains for examining a user's digital identity along with the SA discussed above. Sorting users' SA by creating clusters of socially oriented attributes can help in specifying users' expected ways of disclosing SA.

5.2. Users' SI Domains of Social Attributes on SM

Users' online identity representation contributes to the formation of a digital identity. Users' true identity is disclosed through different layers of socially oriented classifications. This exposure may trigger privacy issues that should not be ignored. Table 3 categorizes users' SA on SM, trying to extract possible variables and identified disclosures on SM, alongside the five social identity domains.

Table 3. SI Domains, Attributes, Variables, and Identified Disclosures on Social Media.

Social Identity Domains	Social Attributes on SM	Variables	Identified Disclosures
Face	user's name, nickname, profile picture, gender, age, address or residence, education, affiliations, job, personal website, friends' network, national or religious identity, class or income, groups of interests and hobbies	Name, Gender, Nationality, Membership, Education, Sexual orientation	actual name (John), gender (M/F), a photograph of the user, membership in a specific group
Frame	user's photograph, address or residence, contact information (email and phone number), affiliations, job, friends' network, national identity, group of interests	Neighborhood, City, Municipality	exact spatial information (x, y), landmark, hashtags, use of a photograph of the place
Time	photographs, education, affiliations, job, user's website, groups of interests	Hours, Minutes, Day, Week, Month	exact temporal information (hh:mm:ss), use of hashtags, use of a photograph with light depiction
Stage	user's photograph, address or residence, contact information (email and phone number), Education, affiliations, job, friends' network, national identity, user's website, group of interests	Combination of both the Frame and the Time Social Attributes	combination of both the Frame and the Time Expected Ways of Disclosure on SM
Activity or Performance	nickname, photographs, education, affiliations, job, user's personal website, friends' network, national or religious identity, class, income, or political orientation, groups of interest and hobbies	Activity, Occupation	exact activity, use of hashtag, exact occupation, use of a photograph doing an activity

The list is extracted by creating wider branches of the SM variables, while the identified disclosures were collected from our previous work [21,81,82] and supplementary bibliography on the field which was used for carrying out our bibliographical review earlier in this paper. More precisely, Table 3 presents the five umbrella social identity domains on its first column, namely Face, Frame, Time, Stage, and Activity or Performance. In the second column, the 18 users' social attributes on social media are sorted based on the five social identity domains. The third column assists in the categorization of the 18 users' social attributes on SM to variables which could be used as descriptions on SM while users opt to represent parts of their online identity. The last column of the table illustrates the potential identified disclosures as examples of representation by an actual user of social media in order to quantify social attributes as a future pointer when designing appropriate tools for measuring users' social attributes. The level of the granularity of the examples varies based on the preferred level of disclosure on behalf of the user on SM.

Users reveal different degrees of granularity of their SI attributes to represent themselves. The most general domain appears in the first column. The higher the degree of the granularity of the information, the more precise the representation of the user. Therefore, the more precise the representation of the user, the more attributes should be filled in the SM profile. These attributes summarize all the possible blanks which users have to complete before representing their online personas. Column 2 represents the attribute-oriented version of social domains, and it includes the respective number of the 18 SA (presented in Section 4). Column 3 turns the findings of SA into variables before observing potential ways of personal information disclosure on behalf of the user. Column 4 functions as a facilitator for our future steps, upon designing the necessary tools for conducting the qualitative analysis of our research.

In a nutshell, including SA from an attribute-oriented point of view enabled our analysis to proceed in observing and recording the expected ways of disclosing personal information to illustrate parts of users' digital identities.

6. Conclusions

6.1. General Remarks

Cloud computing services, such SM, generate new and different flows of information, designating users and affecting how users are self-identified, as well as how others determine them, as complex digital postmodern subjects. Such internal and external identity transformations respectively impact users' privacy management, which is integrally interrelated to the integrity of their identity information, as a self- or socio-constructed series of connected and coherent pieces of information (Wachter, 2018). Users of all ages represent themselves both intentionally, via the necessary procedures of self-determination and self-disclosure [57,58], and unintentionally through SA combination inferences [26,79]. Thus, online identities are shaped due to SM omnipresence imposing further privacy implications within them. Accordingly, software engineers need to be provided with more sufficient tools and methodologies in setting privacy requirements from qualitative data to ensure the optimal design of privacy-aware software systems [78]. Despite the fact that several privacy-enhancing technologies have been developed, the need for a more socio-technical-oriented addressing of identity management within SM has emerged due to the challenges that are related to the accessibility, scalability, and linkability of users' personal information among systems and services. Consequently, an essential challenge for developers and engineers is to provide technical mechanisms that enable both interoperability among systems and services as well as common meanings among users and systems, considering users' social needs and behaviors. These should serve users' preferences for privacy needs.

Even though identity and its management are central issues within SM, previous literature has not yet adequately categorized which identity characteristics and attributes, (Faces, Time) and in which context (Frame, Stage), determine users' behaviors and lead to privacy implications simultaneously. In this regard, the conducted review, drawing on previous literature, identified joint identity characteristics and defined the 18 SA, which not only enable online representations, but also lead to several privacy implications. Understanding the relationships among the social domains, the SA, and social variables in the process of users' representation is crucial to further gain insight into the social aspects imposing privacy implications that should be dealt when designing privacy-aware information systems. Taking into account these SA, developers can provide users with different approaches to protect their subjective privacy preferences, deriving from their self-determination and self-disclosure within SM. Such future steps may concern the designing of a qualitative tool for gathering users' data and a geolocation case study scenario, supporting users' need for realistic depictions [13,30,31,47], so as to ensure their privacy through more socially oriented identity management techniques.

6.2. Limitations and Future Work

Last but not least, it is important to note the limitations of the paper in this subsection of the paper. More precisely, user restriction in filling predefined fields while completing their profiles could have led to restricting the SA of our analysis, creating a limitation to the paper. However, to address this limitation, we extracted SA from research papers on attributes, scales, variables, attributes, users' concerns, privacy risks, and strategies that combined SA and information disclosure on SM. Combining different research papers, we were able to collect users' attributes that might be represented by uploaded content on users' social media accounts, except those that were uploaded using the predefined fields of social media platforms. This content can represent parts of users' online personas in multiple ways which should also be explored. Users' sensitive information is vital to be included as important parts of online identities. Our future steps will also point towards proposing possible ways of handling users' more sensitive attributes. After listing users' 18 SA, researchers will incorporate these attributes in an upcoming tool, intending to better understand and address these kinds of attributes when designing privacy-aware information systems.

Author Contributions: Supervision, C.K. and S.G.; Writing—original draft, K.V.; Writing—review & editing, A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not Applicable.

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

References

1. Almudawi, N.A. Cloud Computing Privacy Concerns in Social Networks. *Int. J. Comput.* **2016**, *22*, 29–36.
2. Kiranmayee, T.S. A Survey on the Role of Cloud Computing in Social Networking Sites. *Int. J. Comput. Sci. Inf. Technol.* **2015**, *6*, 1509–1512.
3. DeHart, J.; Stell, M.; Grant, C. Social Media and the Scourge of Visual Privacy. *Information* **2020**, *11*, 57. [CrossRef]
4. Lenberg, P.; Feldt, R.; Wallgren, L.G. Behavioral Software Engineering: A Definition and Systematic Literature Review. *J. Syst. Softw.* **2015**, *107*, 15–37. [CrossRef]
5. Kalloniatis, C.; Kavakli, E.; Gritzalis, S. Addressing Privacy Requirements in System Design: The PriS Method. *Requir. Eng.* **2008**, *13*, 241–255. [CrossRef]
6. Margulis, S.T. On the Status and Contribution of Westin's and Altman's Theories of Privacy. *J. Soc. Issues* **2003**, *59*, 411–429. [CrossRef]
7. Begel, A.; Deline, R.; Zimmermann, T. Social Media for Software Engineering. In Proceedings of the FSE/SDP Workshop on Future of Software Engineering Research, Santa Fe, NM, USA, 7–11 November 2010; pp. 33–38.
8. Schwartz, R.; Halegoua, G.R. The Spatial Self: Location-Based Identity Performance on Social Media. *New Media Soc.* **2015**, *17*, 1643–1660. [CrossRef]
9. Fusco, S.J.; Michael, K.; Michael, M.G. Using a Social Informatics Framework to Study the Effects of Location-Based Social Networking on Relationships between People: A Review of Literature. In Proceedings of the 2010 IEEE International Symposium on Technology and Society, Wollongong, Australia, 7–9 June 2010; pp. 157–171.
10. Liu, B.; Zhou, W.; Zhu, T.; Gao, L.; Xiang, Y. Location Privacy and Its Applications: A Systematic Study. *IEEE Access* **2018**, *6*, 17606–17624. [CrossRef]
11. Gurses, F.S. *Multilateral Privacy Requirements Analysis in Online Social Network Services*; KU Leuven: Heverlee, Belgium, 2010.
12. Joinson, A.N.; Paine, C.B. *Self-Disclosure, Privacy and the Internet*; Joinson, A.N., McKenna, K.Y.A., Postmes, T., Reips, U.-D., Eds.; Oxford University Press: Oxford, UK, 2012; Volume 1.
13. Marwick, A. *Online Identity in Companion to New Media Dynamics*; Wiley: Hoboken, NJ, USA, 2013; pp. 355–364.
14. Zhou, B.; Pei, J.; Luk, W. A Brief Survey on Anonymization Techniques for Privacy Preserving Publishing of Social Network Data. *SIGKDD Explor. Newsl.* **2008**, *10*, 12–22. [CrossRef]
15. Hogan, B. Pseudonyms and the Rise of the Real-Name Web. In *A Companion to New Media Dynamics*; Hartley, J., Burgess, J., Bruns, A., Eds.; Wiley-Blackwell: Oxford, UK, 2013; pp. 290–307, ISBN 978-1-118-32160-7.
16. Taddicken, M. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *J. Comput.-Mediat. Comm.* **2014**, *19*, 248–273. [CrossRef]
17. Rodotà, S. Privacy, Freedom, and Dignity. 2004. Available online: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293 (accessed on 19 August 2022).

18. Blanco Ramírez, G.; Palu-ay, L. "You Don't Look like Your Profile Picture": The Ethical Implications of Researching Online Identities in Higher Education. *Educ. Res. Eval.* **2015**, *21*, 139–153. [CrossRef]
19. Jenkins, R. *Social Identity*, 3rd ed.; Routledge: London, UK; New York, NY, USA, 2008; ISBN 978-0-415-44848-2.
20. Myles, G.; Friday, A.; Davies, N. Preserving Privacy in Environments with Location-Based Applications. *IEEE Pervasive Comput.* **2003**, *2*, 56–64. [CrossRef]
21. Vgena, K.; Kitsiou, A.; Kalloniatis, C.; Kavroudakis, D. Do Identity and Location Data Interrelate? New Affiliations and Privacy Concerns in Social-Driven Sharing. In *Trust, Privacy and Security in Digital Business*; Gritzalis, S., Weippl, E.R., Katsikas, S.K., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I., Eds.; Springer International Publishing: Cham, Switzerland, 2019; Volume 11711, pp. 3–16, ISBN 978-3-030-27812-0.
22. Vgena, K.; Mavroeidi, A.-G.; Kitsiou, A.; Kalloniatis, C. Can Social Gamification and Privacy Co-Exist? Identifying the Major Concerns. In Proceedings of the 25th Pan-Hellenic Conference on Informatics, Volos, Greece, 26–28 November 2021.
23. Austin, L.M. Re-Reading Westin. *Theor. Inq. Law* **2019**, *20*, 53–81. [CrossRef]
24. Beldad, A.; Kusumadewi, M.C. Here's My Location, for Your Information: The Impact of Trust, Benefits, and Social Influence on Location Sharing Application Use among Indonesian University Students. Available online: https://reader.elsevier.com/reader/sd/pii/S0747563215001685?token=8EA609560A5E713BFE0E4583698789CAF5058ED85DE538327F28BDB6D5F2461EF46A4B750582D43395CD418D29D3D257 (accessed on 29 July 2020).
25. Michael, G.E.K.; Michael, M.G. The Social and Behavioural Implications of Location-Based Services. *J. Locat. Based Serv.* **2011**, *5*, 121–137. [CrossRef]
26. Lahlou, S. Identity, Social Status, Privacy and Face-Keeping in Digital Society. *Soc. Sci. Inf.* **2008**, *47*, 299–330. [CrossRef]
27. Curzon, J.; Almehmadi, A.; El-Khatib, K. A Survey of Privacy Enhancing Technologies for Smart Cities. *Pervasive Mob. Comput.* **2019**, *55*, 76–95. [CrossRef]
28. Wachter, S. Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *Comput. Law Secur. Rev.* **2018**, *34*, 436–449. [CrossRef]
29. Maple, C. Security and Privacy in the Internet of Things. *J. Cyber Policy* **2017**, *2*, 155–184. [CrossRef]
30. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, Privacy and Trust in Internet of Things: The Road Ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
31. Talbot, C.V.; Talbot, A.; Roe, D.J.; Briggs, P. The Management of LGBTQ+ Identities on Social Media: A Student Perspective. *New Media Soc.* **2022**, *24*, 1729–1750. [CrossRef]
32. Emanuel, L.; Stanton Fraser, D. Exploring Physical and Digital Identity with a Teenage Cohort. In Proceedings of the 2014 Conference on Interaction Design and Children, Aarhus, Denmark, 17–20 June 2014; ACM: New York, NY, USA, 2014; pp. 67–76.
33. Satchell, C.; Shanks, G.; Howard, S.; Murphy, J. Identity Crisis: User Perspectives on Multiplicity and Control in Federated Identity Management. *Behav. Inf. Technol.* **2011**, *30*, 51–62. [CrossRef]
34. Papaioannou, T.; Tsohou, A.; Karyda, M. *Shaping Digital Identities in Social Networks: Data Elements and the Role of Privacy Concerns*; Springer: Cham, Switzerland, 2020.
35. Wessels, B. Identification and the Practices of Identity and Privacy in Everyday Digital Communication. *New Media Soc.* **2012**, *14*, 1251–1268. [CrossRef]
36. Miguel, C.; Medina, P. The Transformation of Identity and Privacy through Online Social Networks (The CouchSurfing Case). 2011. Available online: https://eprints.leedsbeckett.ac.uk/id/eprint/2159/1/The%20Transforma (accessed on 19 August 2022).
37. Bria, F.; Primosig, F. Internet as a Common or Capture of Collective Intelligence. Available online: https://dcentproject.eu/wp-content/uploads/2015/06/D3.3-Annex-Internet-Identity-Seminar_annex.pdf (accessed on 19 August 2022).
38. Yuan, M.; Chen, L.; Yu, P.S.; Yu, T. Protecting Sensitive Labels in Social Network Data Anonymization. *IEEE Trans. Knowl. Data Eng.* **2013**, *25*, 633–647. [CrossRef]
39. Papacharissi, Z. *A Networked Self Identity Performance and Sociability on Social Network Sites*; Routledge: London, UK, 2012.
40. 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.* **2018**, *20*, 141–161. [CrossRef]
41. Fei Wu, P. The Privacy Paradox in the Context of Online Social Networking: A Self-Identity Perspective. Available online: https://www.researchgate.net/publication/329039895_The_privacy_paradox_in_the_context_of_online_social_networking_A_self-identity_perspective_JOURNAL_OF_THE_ASSOCIATION_FOR_INFORMATION_SCIENCE_AND_TECHNOLOGY (accessed on 21 September 2019).
42. Kokolakis, S. Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. *Comput. Secur.* **2017**, *64*, 122–134. [CrossRef]
43. Acquisti, A.; Gross, R. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In Proceedings of the Privacy Enhancing Technologies; Danezis, G., Golle, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 36–58.
44. Gross, R.; Acquisti, A. Information Revelation and Privacy in Online Social Networks (The Facebook Case). In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, USA, 7 November 2005.
45. Hoy, M.G.; Milne, G. Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *J. Interact. Advert.* **2010**, *10*, 28–45. [CrossRef]
46. Shafie, L.A.; Nayan, S.; Osman, N. Constructing Identity through Facebook Profiles: Online Identity and Visual Impression Management of University Students in Malaysia. *Procedia Soc. Behav. Sci.* **2012**, *65*, 134–140. [CrossRef]

47. van Dijck, J. 'You Have One Identity': Performing the Self on Facebook and LinkedIn. *Media Cult. Soc.* **2013**, *35*, 199–215. [CrossRef]
48. Zhao, S.; Grasmuck, S.; Martin, J. Identity Construction on Facebook: Digital Empowerment in Anchored Relationships. *Comput. Hum. Behav.* **2008**, *24*, 1816–1836. [CrossRef]
49. Kalloniatis, C. Increasing Internet Users Trust in the Cloud Computing Era: The Role of Privacy. *J. Mass Commun. Journal.* **2016**, *6*, 2–5. [CrossRef]
50. Kalloniatis, C. Incorporating Privacy in the Design of Cloud-Based Systems: A Conceptual Meta-Model. *Inf. Comput. Secur.* **2017**, *25*, 614–633. [CrossRef]
51. Marwick, A.; Boyd, D. To See and Be Seen: Celebrity Practice on Twitter. *Convergence* **2011**, *17*, 139–158. [CrossRef]
52. Albrechtslund, A. New Media and Changing Perceptions of Surveillance. In *A Companion to New Media Dynamics*; Hartley, J., Burgess, J., Bruns, A., Eds.; Wiley-Blackwell: Oxford, UK, 2013; pp. 309–321, ISBN 978-1-118-32160-7.
53. Bazarova, N.N.; Choi, Y.H. Self-Disclosure in Social Media: Extending the Functional Approach to Disclosure Motivations and Characteristics on Social Network Sites. *J. Commun.* **2014**, *64*, 635–657. [CrossRef]
54. Powell, L.M.; Wimmer, H.; Rebman, C. Learner security & privacy risks: How usage of online social media outside a learning management system affects learners' digital identity. *Issues Inf. Syst.* **2019**, *20*, 1–7.
55. Arthur, P.L. Data Portraits: Identity, Privacy, and Surveillance. *Auto/Biogr. Stud.* **2017**, *32*, 371–373. [CrossRef]
56. Beam, M.A.; Child, J.T.; Hutchens, M.J.; Hmielowski, J.D. Context Collapse and Privacy Management: Diversity in Facebook Friends Increases Online News Reading and Sharing. *New Media Soc.* **2018**, *20*, 2296–2314. [CrossRef]
57. Brandtzaeg, P.B.; Lüders, M. Time Collapse in Social Media: Extending the Context Collapse. *Soc. Media Soc.* **2018**, *4*, 205630511876334. [CrossRef]
58. Marwick, A.E.; Boyd, D. I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience. *New Media Soc.* **2011**, *13*, 114–133. [CrossRef]
59. Marwick, A.E.; Boyd, D. Networked Privacy: How Teenagers Negotiate Context in Social Media. *New Media Soc.* **2014**, *16*, 1051–1067. [CrossRef]
60. Hodkinson, P. Bedrooms and beyond: Youth, Identity and Privacy on Social Network Sites. *New Media Soc.* **2017**, *19*, 272–288. [CrossRef]
61. Westin, A.F. Social and Political Dimensions of Privacy. *J. Soc. Issues* **2003**, *59*, 431–453. [CrossRef]
62. Debatin, B. *Privacy Online*; Trepte, S., Reinecke, L., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; ISBN 978-3-642-21520-9.
63. Yuan, M.; Chen, L.; Yu, P.S. Personalized Privacy Protection in Social Networks. *Proc. VLDB Endow.* **2010**, *4*, 141–150. [CrossRef]
64. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews | The BMJ. Available online: https://www.bmj.com/content/372/bmj.n71 (accessed on 29 July 2022).
65. Lutz, C.; Ranzini, G. Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder. *Soc. Media* **2017**, *3*, 2056305117697735.
66. Eastin, M.S.; Brinson, N.H.; Doorey, A.; Wilcox, G. Living in a Big Data World: Predicting Mobile Commerce Activity through Privacy Concerns. *Comput. Hum. Behav.* **2016**, *58*, 214–220. [CrossRef]
67. Vgena, K.; Kitsiou, A.; Kalloniatis, C. Understanding the Role of Users' Socio-Location Attributes and Their Privacy Implications on Social Media. *Inf. Comput. Secur.* 2022; ahead-of-print. [CrossRef]
68. Cover, R.; Doak, S. Identity Offline and Online. In *International Encyclopedia of the Social & Behavioral Sciences*; Elsevier: Amsterdam, The Netherlands, 2015; pp. 547–553, ISBN 978-0-08-097087-5.
69. Ismail, S. An Evaluation of Students' Identity-Sharing Behaviour in Social Network Communities as Preparation for Knowledge Sharing. Ismail, Shahrinaz. An evaluation of students' identity-sharing behavior in social network communities as preparation for knowledge sharing. *Int. J. Adv. Sci. Arts* **2010**, *1*, 14–21.
70. Papacharissi, Z. *A Networked Self: Identity, Community, and Culture on Social Network Sites*; Routledge: London, UK, 2010; ISBN 978-1-135-96616-4.
71. Tufekci, Z. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bull. Sci. Technol. Soc.* **2008**, *28*, 20–36. [CrossRef]
72. Feher, K. Digital Identity and the Online Self: Footprint Strategies—An Exploratory and Comparative Research Study. *J. Inf. Sci.* **2021**, *47*, 192–205. [CrossRef]
73. Birnholtz, J.; Fitzpatrick, C.; Handel, M.; Brubaker, J.R. Identity, Identification and Identifiability: The Language of Self-Presentation on a Location-Based Mobile Dating App. In Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services, Toronto, ON, Canada, 23–26 September 2014; ACM: New York, NY, USA; pp. 3–12.
74. Pempek, T.A.; Yermolayeva, Y.A.; Calvert, S.L. College Students' Social Networking Experiences on Facebook. *J. Appl. Dev. Psychol.* **2009**, *30*, 227–238. [CrossRef]
75. Stutzman, F. An Evaluation of Identity-Sharing Behavior in Social Network Communities. *J. Int. Digit. Media Arts Assoc.* **2006**, *3*, 10–18.
76. Marwick, A. The Public Domain: Surveillance in Everyday Life. Available online: https://www.researchgate.net/publication/279673507_The_Public_Domain_Surveillance_in_Everyday_Life (accessed on 2 March 2019).
77. Papacharissi, Z.; Easton, E. In the Habitus of the New. In *A Companion to New Media Dynamics*; John and Wiley and Sons: Hoboken, NJ, USA, 2013; pp. 167–184, ISBN 978-1-118-32160-7.

78. Li, S.; Li, J.Z. Web and Social Media Dynamics, and Evolutionary and Adaptive Branding: Theories and a Hybrid Intelligent Model. In Proceedings of the 13th international conference on artificial intelligence, knowledge engineering and data bases, Gdansk, Poland, 15–17 May 2014.
79. Nario-Redmond, M.R.; Biernat, M.; Eidelman, S.; Palenske, D.J. The Social and Personal Identities Scale: A Measure of the Differential Importance Ascribed to Social and Personal Self-Categorizations. *Self Identity* **2004**, *3*, 143–175. [CrossRef] [PubMed]
80. Kounadi, O.; Resch, B.; Petutschnig, A. Privacy Threats and Protection Recommendations for the Use of Geosocial Network Data in Research. *Soc. Sci.* **2018**, *7*, 191. [CrossRef]
81. Vgena, K.; Kitsiou, A.; Kalloniatis, C.; Kavroudakis, D.; Gritzalis, S. Toward Addressing Location Privacy Issues: New Affiliations with Social and Location Attributes. *Future Internet* **2019**, *11*, 234. [CrossRef]
82. Vgena, K.; Kitsiou, A.; Kalloniatis, C.; Kavroudakis, D. *Disclosing Social and Location Attributes on Social Media: The Impact on Users' Privacy*; Springer LNCS Lecture Notes in Computer Science: Darmstadt, Germany, 2021; Volume 12501.