USERS' MANAGEMENT OF MOBILE DEVICES AND PRIVACY

Cómo gestionan los usuarios sus dispositivos móviles y su privacidad

Ana Serrano-Tellería

Ana Serrano-Tellería, accredited as associated professor by *Aneca*, is an assistant professor at *Universidad de Castilla La Mancha* and a postdoctoral researcher at *LabCom.IFP*, *University of Beira Interior*, Portugal. Freelancer since 2012 as a media consultant, R+D+i project manager, journalist, and performer. Her research interests are: Corporate and intercultural communication, entrepreneurial journalism, media studies, digital / mobile / online communication and design, performing & stage arts. She has worked as a reviewer for *ICA*, *IAMCR*, *IGI Global*, *iJIM*, *Communication studies*, *Derecom*, *Ciaiq.org*, etc. Full grants received from: *Spanish Confederation of Young Entrepreneurs* with *Spanish Ministry of Employment and Social Security*, *Universidad de Cantabria*, *Sodercan – Government of Cantabria*, *Universidad del País Vasco*, *Federal University of Bahia* (Brazil), *Ministry of Science and Innovation* (Government of Spain), European Union, *Marcelino Botin Foundation*, and *US Embassy* in Spain. Postdoctoral researcher in *Digidoc* (research group on digital documentation and interactive communication) at *Universitat Pompeu Fabra* (Spain) (2017), and in *Digitalmedia*, at *Universidad Carlos III de Madrid* (Spain) (2018).
http://orcid.org/0000-0003-1625-4411

Universidad de Castilla La Mancha, Journalism Faculty
Aulario Polivalente. Campus Universitario. 16071, Cuenca, Spain
ana.serrano@uclm.es

Abstract

This article aims to offer a guide of observed practices based on the main results obtained after the two-year European *Feder* project (April 2013-15) 'Public and private in mobile communications' carried out at *LabCom.IFP*, *Beira Interior University* in Portugal. Both quantitative and qualitative methods were used (surveys, interviews, focus groups, content analysis, digital ethnography, observation ethnography, workshops, etc.) in order to describe how users manage their public, private, intimate and personal spheres within the mobile media ecosystem. Results obtained showed an increased awareness of the risks without a concomitant exploration of consequences, an extensively circumstantial behaviour pattern influenced by interface design and volatile policies, terms and conditions, and a lack of rational user behaviours and performances.

Keywords

Data; Mobile devices; Mobile ecosystem; Mobile phones; Privacy; Private sphere; Public sphere; Intimate sphere; Personal sphere; Smartphones.

Resumen

Este artículo ofrece una guía de prácticas observadas, basada en los principales resultados obtenidos en el proyecto europeo *Feder* de dos años (2013-15) 'Public and private in mobile communications' llevado a cabo en *LabCom.IFP*, *Universidad de Beira Interior* en Portugal. Se aplicaron tanto métodos cuantitativos como cualitativos (encuestas, entrevistas, grupos de foco, análisis de contenido, etnografía digital, observación etnográfica, workshops, etc.). Se describe cómo los usuarios manejan sus esferas públicas, privadas, íntimas y personales en el ecosistema mediático móvil. Los resultados obtenidos mostraron una creciente consciencia sobre los riesgos, aunque sin profundizar en los mismos, un comportamiento altamente circunstancial influenciado por el diseño de la interfaz y por la volatilidad de las políticas, términos y condiciones, así como por una falta de racionalidad en los comportamientos de los usuarios.

Palabras clave

Data; Dispositivos móviles; Ecosistema móvil; Teléfonos móviles; Privacidad; Esfera privada; Esfera pública; Esfera íntima; Esfera personal; Smartphones.

Serrano-Tellería, Ana (2018). "Users' management of mobile devices and privacy". *El profesional de la información*, v. 27, n. 4, pp. 822-829.

https://doi.org/10.3145/epi.2018.jul.11

Artículo recibido el 14-12-2017
Aceptación definitiva: 18-04-2018

1. Introduction

In Adam Alter's *Irresistible*: *The rise of addictive technology and the business of keeping us hooked*, he claims that

> "addiction is produced largely by environment and circumstances" and "Bilton's tech experts also discovered that the environment and circumstance of the digital age are far more conducive to addiction than anything humans have experienced in our history" and "modern tech is efficient and addictive" (**Alter**, 2017, p. 4).

Alter cited Tristan Harris, a "design ethicist", as saying the problem isn't that people lack willpower; it's that

> "there are a thousand people on the other side of the screen whose job it is to break down the self-regulation you have" (**Alter**, 2017, p. 3).

Alter further describes how

> "smart behavioural architects do two things: they design temptation-free environments and they understand how to blunt unavoidable temptations. This process is a bit like taking apart a computer: by reverse engineering the experience, you learn what makes it addictive in the first place, and therefore how to defuse it" (**Alter**, 2017, p. 287).

On the users' side, Alter emphasised that

> "we're now so focused on getting more done in less time, that we've forgotten to introduce an emergency brake" (**Alter**, 2017, p. 6).

Exploring addictions, Alter explained that what substance addictions and behavioural addictions have in common is that they activate the same brain regions and they are fuelled by some of the same basic human needs: social engagement and social support, mental stimulation, and a sense of effectiveness. Specifically, behavioural addictions comprise six ingredients:

> "- compelling goals that are just beyond reach;
> - irresistible and unpredictable positive feedback;
> - a sense of incremental progress and improvement;
> - tasks that become slowly more difficult over time;
> - unresolved tensions that demand resolution; and
> - strong social connections.
>
> Despite their diversity, today's behavioural addictions embody at least one of those six ingredients" (**Alter**, 2017, p. 9)

and

> "obsession and compulsion are close relatives" (**Alter**, 2017, p. 20).
>
> "Phones are disruptive by their mere existence, even when they aren't in active use. They are distracting because they remind us of the world beyond the immediate conversation, and the only solution, the researchers wrote, is to remove them completely" (**Alter**, 2017, p. 16),

which begs the question: how can we users manage this environment and circumstances? Thus, our detailed research questions included:

- Does the amplification of human abilities (diluted along space-time dimensions) and a continuous flow of data alter the implementation of identity in online profiles?
- Are we aware of these changes and are they voluntary?
- Is it possible to achieve a deep level of interaction with people we never meet?
- Will the balance between authenticity and anonymity, privacy and functionality delimit the public, private, intimate and personal spheres?
- What will the scope of the common space be?

In this sense and taking into account the importance of time priority as a variable, an analysis of the concepts of space appropriation, profile, and willfulness are proposed from a perspective that places the Human Being at the center (that is, as a communication portal; **Fidalgo** *et al*., 2013).

2. Users' management of mobile devices and privacy

Bearing in mind this addictive technology, we need to address privacy, which

> "precisely because it ensures we're never fully known to others or to ourselves, provides a shelter for imaginative freedom, curiosity and self-reflection. So to defend the private self is to defend the very possibility of creative and meaningful life" (**Preston**, 2014).

In this article, we will focus on the main results obtained from the methods applied. For a deeper understanding, we recommend an extended state-of-the art review (**Serrano-Tellería** *et al.*, 2014-2017). Our results will be discussed and summed up in three stages:

1) Users' habits & privacy;

2) Managing accounts & privacy; and

3) Managing media & privacy.

A summary of the main results obtained in the 'P&P' project (**Serrano-Tellería** *et al.*, 2014-2017) will be given. A broad view about general uses and habits will be introduced using the quantitative approach offered by surveys: an exploratory one (ES), and three online surveys on: general users and perceptions (GS), personal data (DS) and images (IS).

> "Users remain at a superficial level of awareness and do not delve into the implications of these technologies concerning their data and privacy management"

The variety of user actions, behaviours, knowledge, perceptions and performances will be discussed through qualitative analysis in focus groups: one exploratory focus group (EFG), three adolescents focus groups (AFG) and an adult focus groups (FG); as well as in-person interviews (I) and telephone interviews (IT). Content analysis has been accomplished by comparing the privacy terms and conditions of the mobile applications and platforms most employed by users (PCA). Another was focused on user debates and

image sharing through *Twitter* (TCA), *Reddit* (RCA) and *Instagram* (ICA).

Both digital ethnography (DE) and observation ethnography (OE) were carried out as well. The former was mostly focused on describing the different strategies developed among the members of a *Facebook* group (carpooling), to which the researcher belonged, concerning types of conversations, levels of privacy, selection of contacts, etc. Meanwhile, the latter was focused on user actions, behaviours, and performances with mobile devices in an open public space, the main shopping centre in the city.

The methodologies mentioned were complemented by a hybrid and experimental method developed during a workshop with 44 BA students in Communication (WCA). It consisted of writing an essay at the end of the workshop, based on an open-ended enquiry. It was based on the premise that writing is a suitable method by which to discover users' internalization and understanding of their cognitive and behavioural processes.

> "Users claimed that mobile phones encouraged intrusions on privacy (e.g., when receiving calls from work)"

3. Overall users' habits and privacy

In line with data ethics, Harris (previously cited by Alter), in order to raise users' awareness about, among other elements, *big data*, *dataism*, *the algorithmic self*, *the quantified self*, the difference between *profile* and *digital identity*, *the invisible audiences*, and the volatility of these technologies' terms, conditions, and data policies, I proposed an international ethics code for the interface design of these technologies (**Serrano-Tellería**, 2017a). Users revealed a gap between their awareness of existing and potential risks and their final actions, which may be motivated both by the design of this *addictive* and *irresistible* technology and by the strong connection between it and users' nervous systems (**Serrano-Tellería**, 2017a).

We observed that users are aware of big data and concerned about personal information and about apps' terms, conditions, and data policies. However, they mixed up *profile* and *digital identity*: most did not read conditions and policies (difficult to understand properly and constantly being updated) and followed other users' actions (e.g., installing an application just because others had done so before). This behaviour matches the hypothesis put forward that these technologies promote a lack of rationality and reflection in users. Thus users remain at a superficial level of awareness and do not delve into the implications of these technologies concerning their data and privacy management.

Examples of this behaviour include users' beliefs that privacy depends largely on their ability to control the use made of the equipment, much less, the content saved on their mobile devices and how it is shared on the Internet. Users felt secure just knowing that privacy settings exist and they defended as strategies publishing in closed circles, avoiding location and identification (mainly pictures) and publications of children. In this sense, users are concerned about the data stored on the device and who has access to the data, but they are unaware of the *invisible audiences*, *dataism*, *the algorithmic self*, *the quantified self*, etc. Many users agreed to offer their data for free services without fully acknowledging nor understanding the implications (**Gómez-Barroso**, 2018; **Gómez-Barroso**; **Feijóo**; **Martínez-Martínez**, 2018).

Users claimed that mobile phones encouraged intrusions on privacy (e.g., when receiving calls from work) and described suffering "anxiety" when "having to be always available". They also stated that mobile phones were an integral part of their lives and named benefits, such as being in touch with the people you "care about", making it possible to "manage everyday tasks", and helping to "participate and share collective issues". They also listed as benefits sociability, social coordination (and the maintenance thereof), access to work, and, for older people, security. Mobile phone use was deemed to be strongly circumstantial, and different contexts required different behaviours, with no general rules stipulated by actors (no *negotiation as to what is public and what is private*).

4. Managing accounts and privacy

As for how users deal with personal accounts in relation with privacy issues and settings, in the study we found a wide variety of definitions for *profile*, with confusion between it and *digital identity*. Users included the results of their actions within this idea of 'profile', while not specifically mentioning the digital footprint. The users studied managed between one and fifteen 'profiles', with an average of four. There was considerable variation in (and perceptions of) time spent on mobile phones to manage personal accounts ranging from 15 minutes to 3-4 hours per day.

> "The users studied managed between one and fifteen 'profiles', with an average of four"

In the Exploratory Survey (ES), 55% surveyed did not allow apps to access their contacts or information and 57.7% did not synchronize data with apps. 41.3% surveyed did allow this access and a mere 1% chose "do not know / no answer". To ensure privacy, users deployed strategies like: only sharing with some circles of friends/family; filtering when some publications appeared that they did not want all people to access, including minors; asking for notifications before accepting identification in photos; only uploading photos in which they felt less exposed (e.g., rejecting pictures in swimwear); and not sharing addresses and other more personal data on the network. They perceived how, with more or less direct intervention, the audience seemed to have an effect on the user, influencing the type of content published and its purpose and bearing in mind critical importance, value, the need for acceptance and the need to be visible.

The Personal Data Survey (DS) showed: 60% of mobile phone users used different passwords for different accounts, while 23.1% reported not having a differing set of passwords but used the same one to access various accounts. 51.9% of users changed their passwords and 48.1% did not. As for altering privacy settings, 51.9% did; 31.3% had different settings for different parts; 13.5% had never changed the default settings; and 1.9% did not know they existed.

> 60% of mobile phone users used different passwords for different accounts

During a workshop with 44 BA students (WCA), most "were aware" that once something is published, it is difficult to erase it forever.

Eight directly associated this with the Internet and 12 specifically with social media. Eleven "were aware" that, despite privacy policies, data can be held by others. These "others" could be "friends of friends" and not necessarily direct friends. These others could also be hackers, "malicious persons", "third parties" (i.e. businesses) and *Facebook*. Only one stated that "[privacy] is not as protected as it should be", which pointed towards "alienation".

In fact, *alienation of control* emerged as a theme,[1] particularly with regard to reading privacy policies before installing a new app (adolescents focus groups: AFG). All adolescents admitted to not reading privacy policies and merely clicking on "accept". At the same time, there was an awareness that this behaviour could carry risks and result in manipulation. Regarding *privacy control strategies*, the concept of friendship was very broad and tended to include all acquaintances, indicating that adolescents perceive social media as an extension of their social relationships (**Boyd**, 2014). In terms of *negotiation of the actors* as to what is public and what is private, the idea prevailed that the availability of content was based on an agreement between the people involved, and care was taken not to offend sensibilities.

According to phone interviews (IT), 70% of users installed applications. Those who did not (31%) claimed, above all, that they did not want to give access to their contacts and did not want to be found via location tracking. Only 10% were willing to indicate their location in order to receive personalized advertisements. The majority (61%) did not allow access to location data. Three groups emerged regarding the type of information stored: More than 70% saved 'contact information', 'pictures and videos', 'text messages' and 'applications; between 70% and 40% saved 'e-mail messages', 'notes /voice memos' and 'documents in PDF, *Word*, etc.'; and fewer than a third saved 'websites visited', 'location information', 'passwords' and 'voice mail'. In general, content was not considered "very private", with most falling into the "private" category. The exceptions were 'passwords', which were seen as 'very private', and applications, which were seen as 'not at all private'.

5. Managing media and privacy

As revealed by ES 71%, taking photos or videos was a prominent activity (between one and three times per week) and of the 44 BA students (WCA), one did not take pictures, one did not have a camera phone and five only took pictures when they did not have a camera. The reasons to take photos included being in the company of family and friends, remembering "important dates"; and recording culture and / or travel. According to the IT, 85% of mobile phone users took photos of 'family' and 'travel/holiday'. 60%/70% used phones for photographing/filming 'unexpected situations of everyday life', 'events' and 'meeting friends'. Fewer than 50% were 'self-portraits', photos/filming 'work' or 'mood'.

In focus groups (FG), concern about the dissemination of pictures of themselves had to do with embarrassing situations and the aesthetics of the images. The decision to publish photos in open or closed circles was based on common sense[2]. In the specific case of adolescents (AFG), their *privacy control strategies included*: the strategy of not posting photos, as suggested and reiterated by parents. Adolescents mentioned other strategies: a variation in the range of personal information published; not going beyond basic data like date of birth or high school; not including parents in social networks because of the possible tensions with friends; and showing certain images only in closed groups.

> Most BA students "were aware" that once something is published, it is difficult to erase it forever

According to the survey of images (IS), the perceived risks with respect to pictures placed on the network mainly had to do with the possibility of revealing intimate or compromising situations (61%) and with the possibility of decontextualized images (63%). On the other hand, recognition itself was not a major concern (24%), nor was the identification of others/groups (27%) or habits (38%). In focus group (AFG), some female adolescents specifically highlighted not tagging and / or asking for permission as a way of respecting others and showed awareness of the personal vulnerability inherent in social media. When referring to the method of taking pictures, "place" did not matter "a lot"; –most respondents did not even think about it.

One concern listed (AFG) was the possibility of losing control over the 'image' (self-representation) and, in extreme cases, the possibility of blackmail/bullying. Losing rights to the pictures concerned 47%, but the vast majority gave up this right when uploading/putting photos online. The motivations for sharing suggested that the impetus for interaction was greater than concerns about the risk.

In ES, 68% checked if the app offered "app permission" but 61% did not read those "permissions" before installing. From the concrete DS, 65.4% abandoned apps due to a detected misuse of data, 21.2% chose "I will consider this possibility in the future", 12.5% did not, and 1% chose "do not know,

no answer". As for *privacy control strategies* (AFG): our adolescent respondents had developed a set of weak strategies. Most discarded the use of apps in social media that showed where people were at any given time. The choice to download an app further depended on knowing others who had already done so. The importance of peer behaviour at this stage of the life cycle is also reflected in behaviour when entering the digital world (**Boyd**, 2014).

Returning to the specific DS, 92.3% were registered on social network sites (SNS), with the data sharing distributions shown in Table 1.

66.3% set data visibility and sharing on SNS to be visible only to friends, 15.4% had different data visibility settings for different people, 8.7% were not sure who could see their data, and 8.2% allowed everyone to see it.

In the case of BA students (WCA), 30 (out of 44) felt that the information they shared was not secure, three felt that it was; and the rest said that it depended. Users were aware of some risks but did not explore their potential dangers.

> 65.4% abandoned apps due to a detected misuse of data

Delving into *privacy control strategies* (AFG), adolescents were aware that access to SNS should be made on trusted devices, taking care to log out. Adolescents also showed concern for what they published, preferring trivialities that do not compromise them. Some adolescents only used accounts and publications for a very restricted circle of friends. Sending/accepting invitations dealt with people they knew, at least by sight. Awareness was prevalent, but it was not linked to the risks inherent in using social media. Thus, this awareness did not lead to use of appropriate behaviours to protect their privacy. At the WCA with 44 BA students, the verbs, nouns and syntax employed indicated the students were used to disclosing privacy and had developed a routine for the process of exposing personal information.

In the exploratory focus groups (EFG), respondents showed awareness of risk in exposing personal aspects that may stay online indefinitely, but their daily practices seemed to reflect little concern. When asked through the DS if they regretted disclosing personal data, 65.9% answered 'no', 15.4% said 'yes' on SNS and 17.8% said 'yes' when shopping online. As for their use of tools for data protection, 85.1% chose 'no', 13.9% chose 'yes, and 1% chose "do not know / no answer". Concerning *invasion of privacy* (AFG): the majority of adolescents referred to pictures posted by parents and in which they were tagged.

Regarding the level of concern with the lack of control over data (DS), users were 'rather concerned' (31.3%), 'worried' (30.3%), 'a little worried' (28.2%) or 'not worried' (9.19%). The reasons they provided for this concern or lack thereof included:

- a belief that the inner SNS structure hinders control over personal data (54.8%);
- difficulty setting up the privacy of their personal data (16.3%);

Table 1. Data sharing distributions

Type of data	%
Basic information	73.6
Contact information	13.9
Personal interests	43.8
Education and training	58.7
Work/job information	36.1
Shared trips	34.6

- not having time to set up privacy of their personal data (16.3%); and
- 'other' (12%).

Asked if companies should store data and for how long, 66.3% said they should not save data, 24% answered for one year, and 18% said indefinitely.

24% made bank transactions online, 75.5% did not, and 0.5% chose "do not know, no answer". On access to data by security agencies, 54.3% agreed only with a legal foundation; 38% did not agree at all; 7.2% agreed on a case-by-case basis; and 0.5% chose "do not know / no answer". Delving into the issue in IT, most users believed that search engines, telephone operators and secret services (government agencies) must store the information for only one year. However, the secret service was often given more time; 35 respondents and two respondents said three and five years respectively.

Regarding the control of their own information and publications, 22 / 44 BA students (WCA) felt they did not control the information available about them, whereas 8 felt that they did control their information. All showed concern about who controls the information –themselves or others- and especially about what others could publish about them and about the appropriation of personal information without their permission.

> *Facebook* was mentioned several times as the "profile" that displays the most data, because it requires users to provide this information

In personal interviews (I) about transparency with regard to storage policies / disclosure to third parties of the data stored on social networks or email accounts, some claimed that these procedures were an invasion/violation of their privacy; others appreciated that, in some cases, the information could be useful and even considered that there should be such monitoring by the authorities, especially when a crime is suspected. One specifically mentioned that this "surveillance" –'Big Brother'– came from the beginning of the century.

Throughout the WCA with BA students, *Facebook* was mentioned several times as the "profile" that displays the most data, because it requires users to provide this information and / or because of its interactive nature. One (out of 44) thought *Facebook* was more secure because it had more privacy settings and only one established a relationship be-

tween publications and personal data. During the EFG, high tolerance for invasion/harassment and unauthorized commercial use of personal data was considered. On this point, users showed an initial awareness of the different sources that collected their personal data. However, studies show that the possibilities –technical settings- concerning profile and digital identity are wider than they may seem (as pertains to how the different applications, platforms, webs, etc., collect and use personal data through an interface design that, as introduced previously, promotes addiction to disclosure as well).

In the specific case of a digital ethnography of a *Facebook* group (carpools) (DE), the following strategies were observed: public availability but publications only from members accepted by administrators; member notifications on their profile pages allowing members to change this option to block notifications; and travel arrangements via private message and without revealing phone numbers (although some people did not care and disclosed their personal contact information in the group). Some group members were not embarrassed about making comments in the group and did not worry that other members were reading these comments. During the trips, the observer-researcher realized that the publication of offers and requests for managing the meetings to arrange the trips was a last resort, and people first called nearby contacts by phone.

Moving onto the analysis of *Twitter* (TCA), *Reddit* (RCA) and *Instagram* (ICA): by classifying the tweets by *Netlytic* and gaining subsequent confirmation by analysing them, it can be concluded that the hashtags *privacy, digital identity* and *username* had a more technological content, while the ones collected for *profile* and *anonymity* were more personal. It was noted that large numbers of messages associated with the hashtag *anonymity* were directly or indirectly related to the *Tor project* (anonymity network).

> In the case of *Instagram*, viral, commonly-used hashtags were employed in many cases to 'promote' images rather than because they were linked to the topic itself

After analysing the tweets collected for *mobile, social media* and *self*, it was concluded that the content shared via *mobile devices* were essentially articles, news or applications sent to provide warnings or to help to protect data on mobile devices. In *social media,* it was observed that most served to share articles and pages on how to improve presence on social networks, both in a marketing context and for "personal promotion" or, in the case of *privacy*, for controlling the levels of privacy settings on social networks. Finally, in analysing *self*, most tweets were photographs (selfies) shared by users on the network through applications like *Instagram* (78%) or social networks (22%). It ought to be highlighted that, in the case of *Instagram*, viral, commonly-used hashtags were employed in many cases to 'promote' images rather than because they were linked to the topic itself.

The messages of a more personal nature, e.g., those discussing actual cases of users' day-to-day lives instead of simply sharing content such as articles or news, were on Reddit, got more interaction than other topics**.** The topics that created the most controversy among users were those related to privacy and anonymity, where it was possible to make a clear division of users into two groups with opposing views. Conversations that generated particular controversy addressed the improper use of individuals' photographs or discussed *Facebook* as an attack on users' privacy.

The analysis of the user accounts on *Instagram* revealed a 'diary' of the users' lives –for instance, one user used *Instagram* to follow a diet and share the results with the audience– mixing moments with friends, family and professional goals. That is to say, users created diaries of their daily lives (different moments of the day) through their *Instagram* accounts.

> Interface design, ever-changing environments and fluid circumstances serve to encourage user addiction and supply rationale behind the otherwise contradictory behaviour observed

6. Conclusions

The technologies studied offer everything users need to become addicted: social engagement, social support, mental stimulation and a sense of effectiveness. Moreover, interface design, ever-changing environments and fluid circumstances serve to encourage user addiction and supply rationale behind the otherwise contradictory behaviour observed.

The inherent contradictions in user behaviour show that users have concerns about privacy while also revealing high tolerance to invasion, harassment and unauthorized commercial use of personal data leading users not to employ the necessary privacy protection strategies (e.g., some users have an idea of the risks of exposing personal data but answering "no" when asked if they regret disclosing it and / or not employing specific tools for protection; or users checking if an application offered 'app permissions' but not reading the policies before installing the app).

An increased awareness and idea of the risks involved was observed, but users generally continued to lack proper abilities and capacities to manage their privacy consciously and properly. Although users deployed a series of strategies to manage and control their privacy (mainly associated with the 'privacy settings' of the applications, devices and platforms) avoiding synchronization, refusing access to contacts, location, and identification tagging in images, controlling member and/or friend requests, and establishing circles and groups to share the information with, these strategies are insufficient. Users "felt secure" just knowing that these 'settings' are available, even though, as experts note, these settings are not enough to protect users' privacy.

General users seemed to be unaware of the implications of these devices (apps, tools, platforms) as features and parameters that shape their online and offline identities (*big data*, *dataism*, *algorithmic self*, *quantified self*, etc.). For example, users considered that the applications installed on their devices are "not at all private" when they collect a great deal of personal information. Users also showed a deep ignorance about the differences between '*profile*' and '*digital identity*'. Thus, a greater understanding of the '*digital path*' and the '*invisible audiences*' should be encouraged in order to raise awareness that the information users provide, both voluntary and involuntary, may provide access to information and/or content to audiences for which that information and/or content was never intended to.

Throughout our study there were different notions and perceptions about what privacy is, particularly in light of the fact that most users' worries were about who and how their content and data were accessed. Users showed different levels of awareness but they were generally in favour of sharing and visibility, even when they claimed to be worried about losing control of the construction of their 'public image's. This situation is exacerbated by difficulties in properly understanding the technology and / or by having to be always available and / or efficient, which all affect the time required to analyse the environment and circumstances surrounding privacy policies and implementation.

> The strategies deployed by users to manage and control their privacy are insufficient

Users seemed to be constantly negotiating the public, private, intimate and personal spheres in everchanging contexts, a liquid media ecology and unstable technological environment. Users are constantly managing their spheres without clear norms because both audiences and contexts may constantly and quickly change altering, consequently, the parameters employed to stablish the required delimitations (e.g., a new audience may enter into the scene, creating new interactions, sharing of contents, etc., generating, as a result of, that a situation and/or content may be considered public, private, intimate, personal, or even a mixed one). In this sense, the hypothesis of the liquid spheres or constellations of spheres were already introduced (**Serrano-Tellería**, 2015c-2017) to describe how users deal with this liquid media ecology and technological environment.

Future topics for consideration include users' *alienation* (as a result of users becoming used to disclosing personal information) and users' disregard for consequences (e.g., motivations for sharing, impetus for interaction, are greater than user concerns about risks). Also, another one includes promote knowledge about differences between '*profile*' and '*digital identity*', and awareness about consequences and implications of *big data*, *dataism*, *algorithmic self*, *quantified self*, etc.

Notes

1. All themes (in *italics*) emerged after applying the thematic analysis method during the three AFG.

2. Sound and prudent judgment based on a simple perception of the situation or facts (by *Merriam-Webster*).

> Users showed a deep ignorance about the differences between '*profile*' and '*digital identity*'

7. References

Alter, Adam (2017). *Irresistible. The rise of addictive technology and the business of keeping us hooked.* New York: Penguin Press. ISBN: 978 1 594206641

Boyd, Danah (2014). *It's complicated. The social lifes of networked teens.* Yale New Haven and London: University Press. ISBN: 978 0 300166316

Fidalgo, António; **Serrano-Tellería, Ana**; **Carvalheiro, José-Ricardo**; **Canavilhas, João**; **Correia, João-Carlos** (2013). "Human being as a communication portal: The construction of the profile on mobile phones". *Revista latina de comunicación social*, n. 68.
https://goo.gl/LSXYgG

Gómez-Barroso, José-Luis (2018). "Uso y valor de la información personal: un escenario en evolución". *El profesional de la información*, v. 27, n. 1, pp. 5-18.
https://doi.org/10.3145/epi.2018.ene.01

Gómez-Barroso, José-Luis; **Feijóo, Claudio**; **Martínez-Martínez, Inmaculada J.** (2018). "Privacy calculus: Factors that influence the perception of benefit". *El profesional de la información*, v. 27, n. 2, pp. 341-348.
https://doi.org/10.3145/epi.2018.mar.12

Preston, Alex (2014). "The death of privacy". *The guardian*, 3 August.
https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston

Serrano-Tellería, Ana (2014). "Interface design on mobile phones: The delimitation of the public and private spheres". In: Paiva, Francisco; Moura, Catarina (orgs.). *Designa: Interface: Intl conf on design research.* Portugal: LabCom, Beira Interior University, pp 87-108. ISBN: 978 989 6541415
http://www.designa.ubi.pt/en/2013

Serrano-Tellería, Ana (2015a). "Emotion and mobile devices". In: Paiva, Francisco; Moura, Catarina (orgs.). *Designa: Desire, intl conf on design research.* Portugal: LabCom.IFP, Beira Interior University. ISBN: 978 989 6541811
https://www.labcom-ifp.ubi.pt/book/253

Serrano-Tellería, Ana (2015b). "The role of the profile and the digital identity on the mobile content". In: Aguado, Juan-Miguel; Feijóo, Claudio; Martínez, Inmaculada J. (eds.). *Emerging perspectives on the mobile content evolution.* IGI Global, pp. 263-282. ISBN: 978 1 466688384
https://doi.org/10.4018/978-1-4666-8838-4.ch014

Serrano-Tellería, Ana (2015c). "Liquid spheres or constellations: Reflections towards mobile devices". In: Carvalheiro, José-Ricardo; Serrano-Tellería, Ana (eds.). *Mobile and digital communication: Approaches to public and private*. LabCom Books. ISBN: 978 989 6542375
http://www.livroslabcom.ubi.pt/book/141

Serrano-Tellería, Ana (2016). "Liquid communication in mobile devices: Affordances and risks". In: Baggio, Bobbe G. *Analyzing digital discourse in virtual modern environments*. IGI Global. ISBN: 978 1 466698994
https://doi.org/10.4018/978-1-4666-9899-4.ch011

Serrano-Tellería, Ana (2017a). "Innovations in mobile interface design: Affordances and risks". *El profesional de la información*, v. 26, n. 2, pp. 320-327.
https://doi.org/10.3145/epi.2017.mar.19

Serrano-Tellería, Ana (2017b). "Twitter na partilha de estratégicas e ferramentas para a privacidade" (Twitter in strategic tools for sharing and privacy). In: Camponez, Carlos; Bruno, Araujo; Miranda, João; Basílio-de-Simões, Rita; Silvia, Santos (eds.). *IX Congresso Sopcom: Comunicação e transformações sociais* (v. 1). ISBN: 978 989 9984004
http://www.bocc.ubi.pt/pag/sopcom/1-ix-congresso.pdf

Serrano-Tellería, Ana (2017c). "Reddit no fluxo das conversas sobre privacidade" (Reddit in the flow of conversations on privacy). In: Camponez, Carlos; Bruno, Araujo; Miranda, João; Basílio de Simões, Rita; Silvia, Santos (eds.) *IX Congresso Sopcom: Comunicação e transformações sociais* (v. 3). ISBN: 978 989 9984035
http://www.bocc.ubi.pt/pag/sopcom/3-ix-congresso.pdf

Serrano-Tellería, Ana (2017d). "Memórias mediadas: Um diário no Instagram" (Mediated memories: A diary on Instagram). In: Camponez, Carlos; Bruno, Araujo; Miranda, João; Basílio-de-Simões, Rita; Silvia, Santos (eds.). *IX Congresso Sopcom: Comunicação e transformações sociais* (v. 2). ISBN: 978 989 9984011
http://www.bocc.ubi.pt/pag/sopcom/2-ix-congresso.pdf

Serrano-Tellería, Ana (ed.) (2017e). *Between the public and private in mobile communication*. Routledge studies in new media and cyberculture. Routledge: New York. ISBN: 978 *1 138225558*
https://www.routledge.com/Between-the-Public-and-Private-in-Mobile-Communication/Telleria/p/book/9781138225558

Serrano-Tellería, Ana; **Branco, Maria-Luísa.** (2015). "Educação para a privacidade no espaço digital: de subsídios para uma proposta curricular". In: Carvalheiro, José-Ricardo (org). *A nova fluidez de uma velha dicotomia: Publico e privado nas comunicações móveis*. Covilhã, Portugal: LabCom books, University of Beira Interior, pp. 107-122. ISBN: 978 989 6542122
http://www.livroslabcom.ubi.pt/book/133

Serrano-Tellería, Ana; **Branco, Maria-Luísa**; **Guimarães, Sandra-Carina** (2017). "Educating for privacy in the digital and mobile ecosystems: toward a proposed syllabus". In: Serrano-Tellería, Ana (ed.) (2017). *Between the public and private in mobile communication*. Routledge Studies in New Media and Cyberculture. Routledge: New York. ISBN: 978 1 138225558
https://www.routledge.com/Between-the-Public-and-Private-in-Mobile-Communication/Telleria/p/book/9781138225558

Serrano-Tellería, Ana; **Oliveira, Marco** (2015). "Liquid spheres on smartphones: The personal information policies". *International journal of interactive mobile technologies*, v. 9, n. 1.
http://online-journals.org/index.php/i-jim/article/view/4065

Serrano-Tellería, Ana; **Pereira, Pedro** (2015). "*Instagram* e a visibilidade das imagens dos utilizadores". In: Carvalheiro, José-Ricardo. *Público e privado nas comunicações móveis*. Coimbra, Portugal: Minerva Coimbra, pp. 297-316. ISBN: 978 972 7983582

Serrano-Tellería, Ana; **Portovedo, Sara; Albuquerque, Ana-Isabel** (2015). "Negociações da privacidade nos dispositivos móveis". In: Carvalheiro, José-Ricardo. *Público e privado nas comunicações móveis*. Coimbra, Portugal: Minerva Coimbra, pp. 119-158. ISBN: 978 972 7983582