Liquid Spheres on Smartphones: The Personal Information Policies

http://dx.doi.org/10.3991/ijim.v9i1.4065

A. Serrano Tellería, M. Oliveira
Beira Interior University, Covilhã, Portugal

Abstract—**Data collected from the profiles and the digital identities has become a valuable currency for the mobile ecosystem, especially between users and providers. Services that required them are also described as the ground floor in direct linked with the infrastructures and as intermediate layers between networks, platforms and applications. The frontier debate between innovation and protection of privacy is shown off undefined and unstable. Therefore, a comparative analysis between 'Privacy Terms and Conditions' as well as the interrelation between operative systems (Apple iOS, Android, Blackberry and Windows Phone), social media platforms (Facebook, LinkedIn, Twitter and Google +) and applications (Instagram, WhatsApp, Line and Vine) were carried out focusing on Privacy issues. Two main tendencies were appreciated in relation with the two principal operative systems: Apple iOS closed environment and Google Android open source. They reconfigured the functional structure and design of platforms and applications in different ways. The liquid spheres observed varied from the first approach that tried to control every action and personal information from the binomial operative system-device and the second one that allowed the user actions and information to be more susceptible to interact with any kind of applications and platforms while the system was linked to information aggregation services to collect the data. Prominent aspects were the various stages of synchronization between the different levels of personal information (contacts, profile, digital identity and localization). Focusing on the case of Portugal, other complementary conclusions obtained from focus group and surveys showed a strong circumstantial pattern behaviour and a concern about privacy issues taking care of some actions while admitted checking if they had the terms and conditions involved - which were too ambiguous - but not reading them. Described also by other international previous researches, they showed lack of rationality in some attitudes and performances as well as limitations on the extension between knowledge and action.**

Index Terms—**Liquid Spheres, Operative Systems, Privacy, Terms and Conditions, Smartphones.**

I. AN UNDEFINED AND UNSTABLE ENVIRONMENT

The delimitation of the public and private spheres in the construction of the different profiles and the digital identities through smartphones on the Internet, especially with the expansion of the different type of applications and social media, has become a focus of attention both from providers and users perspective. It ought to be considered the ever-changing privacy policies of the platforms and the applications, the increasingly requested synchronization of different types of data between the operative systems and its environments, the applications and the platforms[1], the geo-localization, the emergence of companies to safeguard privacy, of platforms and apps that run the contents of others in order to improve the personal image –for example, the content curators-, to promote anonymity and to build on anonymous profiles. Therefore, the data flux in a continuum and diluted paths that reflects this undefined and unstable environment.

This uncertainty may be described from a technological perspective by the tension emerged between the willing to promote innovation and to protect user's data since mobile services –which stated to require this type of information to improve its services- are described as the intermediate layers between networks, operative systems, applications and platforms [1].

On the other hand and from a theoretical perspective, the tension arose between the transformation of people into merchandise [2] and the 'Right to be Forgotten', that European Commission is working on, specially focused on assignment an expiration date for personal data that should be applicable in the specific context of social networks. It occurs in a society where a "curious reversal" redefined the private sphere characterized by the right to confidentiality as a sphere that has become prey to the right to publicity [3]. Concerning policies, there exist two main tendencies: Europe's undefined one trying to control the market and USA and Asia letting it freewill and following the model of testing in progress.

Remembering Wellman's concept of portal[2] [4] applied to Human Being process of communication by smartphones, users exist in a timeless time [5] that is framed by the possibility of the perpetual contact [6] and in a kind of virtual configuration of the online space where the directionality and the distance are confused or undefined [7]. Moreover, in this undefined and unstable mobile ecosystem, users generate an ever-changing profile and digital identity, both conscious and unconsciously, as they have to deal with the liquid spheres constantly to be negotiated.

II. THE LIQUID LIFE AND THE SMARTPHONES

Characteristics that described Digital Media were focused on the constant negotiation of rules where norms and values were not clear, on being a decentralized model with a multimedia and flexible format –constantly chang-

[1] Platforms referred to Facebook, Twitter, LinkedIn and Google +, while the environment (that may also be called platform) related to Apple iOS, Google Android, Blackberry and Windows Phone as operative systems with its relation to apps and mobile services.

[2] "It was I-alone that was reachable wherever I was: at a house, hotel, office, freeway or mail. Place did not matter, person did. The person has become the portal"[4].

ing, updating, correcting and being revised -, where content was insensible to distance and nonlinear, as well as on diverse resources fonts with fragmented audiences whose feedback were so valuable to bear in mind [8]. Those are intertwined with Bauman's metaphor of modern life, so liquid life: fluidity, transience, reticularity and dissolution of borders or boundaries defined [9].

Therefore, the characteristics of Digital Media are liquid ones as none of its frontiers are delimited and they are constantly being negotiated. Even more, the same delimitation might be considered as useless if bearing in mind that the content flows on diverse resources fonts and fragmented audiences –willing to expand-.

Concerning the process of communication by smartphones, the state of perpetual contact [6] enables people to recreate a network of protection similar to that of traditional societies [10], where people maintain a nomadic intimacy within a social system based less on location and more on themselves, so one can stay in touch on the go [11]. "This create a kind of nomadic intimacy in which the public space is no longer a full itinerary, lived in all its aspects, stimuli and prospects, but is kept in the background of an itinerant 'cellular intimacy'" [11].

More than any other media, stated Fidalgo [12] following Geser[3], is the mobile phone that restores the social relations typical of the small communities, a "throwback to pre-modern models of social life" [13].

In this trans-spatial communalism, individuals are losing the habit and confidence to think and decide for themselves due to the umbilical cord that keeps them connected - although physically far - to the original community. Nowadays, this permanent and ubiquitous connection is the cause of much tutored thought [12].

The mobile phone was described as the 7th Mass Media by Ahonen [14] because: It is the first personal mass media, it is permanently carried, it is always on, it has a built-in payment mechanism, it is available at the point of creative inspiration, it has the most accurate audience measurement, it captures the social context of media consumption and it offers a digital interface to the real world. But, as Katz summarized [15], mobile communication improves several dimensions of freedom and increases our choices in life, while it may also be turned against the user: invading personal privacy and causing emotional, political and technological distress.

The spheres liquidity favours the data recollection of personal information since perpetual contact and ubiquity may entail tutored though and lack of behaviour autonomy – for example, when users accept terms and conditions without reading them, just because other people did it before -. The nomadic and cellular intimacy 'on the go' is constantly delimiting the sphere boundaries in this diluted and unstable ecosystem. Too much effort is required from users to be properly updated and to know how to deal with technology, even more, when it is ever-changing. Furthermore, emotions are also liquid, as a result of managing permanent feelings and impulses as well as emerging motivations to be fulfilled.

Therefore, delimiting the different spheres is closely tied to the ability to manage wilfulness, taking into account the importance of the temporal priority as a relevant variable in the process. Also, the balance between the authenticity and the anonymity, the privacy and the functionality are considered key elements trying to distinguish what may be defined as public or private. Moreover, the game between the obscurity and the hyper-visibility that allows users to reach the spotlight of attention and the scope of the common space ought to be considered [16].

III. THE LIQUIDITY BETWEEN THE PUBLIC & THE PRIVATE SPHERES

If remembering Goffman (1959) description of the daily life performance, - where people move between the front-stage and the back-stage, between the public and the private spheres -, the integration of remote communications may be underestimating the importance of face-to-face interactions [17] and undermining the traditional rituals of separation in the different spheres of life [18].

In the emergence of the industrial capitalism and accelerated growth of metropolises of the nineteenth century, the representation of the individuals in public was no longer primarily a mechanism of social identification but also to be - and essentially – producer of personal meanings about each subject [19]. Thus, when and where the change between action and character as appearance occurred? The visual presentation stepped to be invested with meanings associated to personality. Under these conditions, the public system is expressed and transmuted into a system of personal representations. The personality in public considered - widespread belief - that appearance is an indicator of character, which results in the private individuals' anxiety [19].

A situation framed by the fact that electronic audio visual media were increasingly bringing elements of the individual "back-stage" for a facade region, favouring the expression of personal characteristics and exposing areas that before were private [20]. In the world of Goffman [21], people behaved but had no experience [19] where the media was converting the private space into merchandise [20]. Remembering McLuhan, the medium is the message and, it seems even more on the mobile devices, the (pro) consumer – (active) user has become the merchandise.

Bauman's metaphor of the liquid life - fluidity, transience, reticularity and dissolution of borders or boundaries defined -, consistent with the logic of the consumer society, provides a useful counterpart to address some of the characteristics of the mobility. Beyond the correlation between the impact of the digital technology and the digital features of the liquid society (which refers to the reflections on the acceleration, the dislocation, the consumption and the role of identity), the mobile medium particularly fits the parameters of fluidization of technological, institutional and cultural dimensions of the medium previously described by McQuail [22], [1].

IV. CHARACTERISTICS AND STRUCTURE OF THE MOBILE DEVICES

The dissolution of the link between content and support, which had been the basis for the definition of genres and formats, reaches its peak with the expression of the distribution models based on storage services and cloud sync. The mobile environment is, in essence, a multi-device one, whose core lies in a conception of the mode of consumption and access to the content and services.

[3] Sociology of the Mobile Phone. University of Zürich. Online publications. Consult 18 February 2014. URL [http://socio.ch/mobile/]

The ubiquity, the diversification and the intertwining of the consumption scenarios, with a marked tendency towards transversal use of the media and access modes (multi-use), as well as its insertion into social dynamics where real identity games become objects of consumption; redefines the value perception of the contents by the users and converts them into a valuable source of the new resource of the digital economy: the personal information.

Focusing on smartphones, both Apple-iOS and Google-Android laid the basis for the environment – platform – (services, features and content) grouped around an app store, led either by an operative system – Google Android - or by the binomial terminal-operative system – iOS iPhone/iPad -. While Apple leads from its devices, Google does it based on an operative system linked to information aggregation services.

Apple relies on the tight control of their customer databases, which sells content and apps through iTunes and the App Store. Google also sells both through its Google Play Store, but its main bet does not need so much explicit information about the users, who become audiences for the commercial communication that handles Google and its technologies of contextual and behavioural targeting [23].

Both sell content, services and advertising to advertisers, but the formula for success is based on combining the three elements in different proportions and presentations, and this also leads to attract around nuanced public with different experiences. For example, studies tend to appreciate that iPhone users spend more money on their data plans and more time on Social Media that the owners of Android smartphones with similar performance [24] in [1].

Operative systems delimit programming environment, mobile platforms, user interface and experience as well as being the norm to which apps developers, providers and distributors ought to stick to. Amazon Android and Apple iOS prohibit access to rival shops. Meanwhile, platforms group the relation between the different actors through channel and services content distribution, configuring the app stores.

Thus, in addition to including specific relationships (usually external and often strained) with network operators; mobile platforms articulated hardware access (mobile and / or fixed), the operative systems and its user interface, a content management software / applications and a software development kit (SDK) with language and programming parameters specific to the environment – platform -. The content management software / applications also serves as a control of user activity, gathering information on the profile and preferences and limiting forms of income and execution in order to minimize the integration of foreign content to the platform [1].

V. THE PERSONAL INFORMATION

The use of personal information adds value to advertising (discriminated and targeted), is the basis of business models and a clear challenge to the ones of traditional content industries, offering information about users behaviours. Therefore, this raises important questions about privacy and transparency, as well as cookies tracking and data mining. In this environment, consumer protection laws are in a changing and challenging context, where it may be distinguished two main tendencies: USA and Europe.

OECD Privacy Guidelines[4] have described personal information as the information that relates to an individual identified or identifiable. There is some controversy about providers and users on the one hand and, on the other, administrations where are the limits of what is strictly personal information. A restricted conception covers the "who we are" personal data such as name, address, identification, financial records, sanitary ware, etc. A broader concept does the "what we do" behavioural data such as search, navigation, shopping, etc.; and “how, where and when we do”, usage habits such as location, time, frequency, time spent, and so on [1].

A. The Profile and the Digital Identity

A profile is structured information about the users of digital services. Its concrete structure depends on the way the information has been gathered, the technology involved, the types of data or what the law allows. In the mobile ecosystem, this profile is usually richer than in the generic case of Internet and also is linked more clearly – mobile identifier device to the IP address - with a particular individual. Moreover, in the case of having ambient intelligence (context-awareness), the user profile may even include biophysical parameters, charge level of the battery and a rich set of variables on the environment; what may include, in addition to the location and the orientation, temperature, humidity, noise, etc. [1].

Especially mobile technologies show the biggest challenges regarding the use and the abuse of personal information. Main examples are location, and its access to Wi-Fi. A compilation of information that suppliers of the major mobile platforms, Apple-iOS and Google-Android argue that is done to accelerate the provision of different services based on the user's position [25]. According to the theory of multilateral markets, the use of personal information has become a bargaining chip between users and providers, where a strategic relationship occurs between agents involved in the platform: providers, users and advertisers.

The concept of Digital Identity (ID) arises from the combination of three main factors [26]: the concrete manifestation of the self-image of the person on the digital service in question (a professional social network, for example), the elements arising from the protection / limitation / modification or concealment of certain information that users consider according to their preferences (highlight certain employment) and the implementation of policies regarding provider data (creating a unique user ID and log all activities that occur when accessing the social network in question). Therefore, a certain individual may have multiple digital identities.

In structuring information about the users profile and combining the three factors to obtain the possible multiple digital identities, the liquid spheres are once again representative. The personal data flux in an environment supported by the norms of platforms, applications and other

[4] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Consult 28 February 2014.
URL
[http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm].

services, each one with their own market interests and their programming code.

B. *Concerns about Privacy*

At this point, several researches showed the users concerns about privacy but they were not willing to pay for their protection in the case of UK [27] or even willing to sell it. A study indicated that 32% of Canadians would be willing to sell their digital data to the right company for the right price and 45 % would sell at least some of it[5]. Both focused on the fact that it was neither provided information nor tools to ensure contextual integrity, being the use of it out of context what most worries. Contextual integrity refers to the use of personal information in the specific context of the service employed and not outside the concrete relationship established between supplier and consumer [28].

In the USA, findings from January 2014 survey at Pew Research[6] manifested an increase of 7% in information stolen from 2013, with 18% of adults recognizing it as important ones and 21% of them with an email or social networking account being compromised. Half reported becoming more worried about the amount of personal information available online since 2009 (33%). About anonymity in September 2013[7], 86% took steps online to remove or mask their digital footprints and 55% to avoid observation by specific people, organizations, or the government.

Continuing with the case of Canada, many of those who participate in social networking used these spaces to create profiles expressly for public distribution. At the same time, and according to Dr. Burkell[8], the potential hazards of sharing personal information online – from concrete risks such as identity theft to more esoteric risks such as the erosion of personal autonomy as a result of surveillance – were too remote to influence their decisions; especially, when compared with the immediate and tangible benefits of that same sharing.

This is especially true when the collection, sharing and analysis of the personal information occurred invisibly, without our consent or even our knowledge. “Quite frankly, from an individual perspective, we still feel – many of us – as if we have privacy. And on a day-to-day basis … the kind of surveillance we’re under, the kind of oversight we’re under is not evident to us,” commented Dr. Burkell, “The risks we are running are not risks that are immediately evident to us”.

Feijóo and Gomez-Barroso [1] explained two main tendencies to reduce privacy risk: by design and by law. Regarding technology, the PET (technologies enhanced privacy) may help to rebalance the relationship between users and providers, extracting general patterns of consumption and protecting the particular information. Other possibility will be that users may move their data between suppliers, portability of personal data, which would help to reduce the market power of these providers with respect to users, increase competition and, ideally, facilitate services that appeared more respectful with the use of personal information to prevent leakage of users to other suppliers.

These advances must be accompanied by a regulatory framework. There appear to be conclusive user’s lack of rationality when confronted with digital services that are based on the personal information provided by them. To establish and implement the necessary regulation faces considerable challenges: the balance between the innovation and the consumer protection, the risks associated with invasion of privacy in the short, medium and long term and the fact that personal information is handled and transferred in a globalized world where geographic boundaries are irrelevant.

In Europe, the debate is still pretty theoretical without a stable regulatory framework, debating the ‘Right to be Forgotten’ by the European Union. Meanwhile, USA and Asia are leaving the market to dominate this debate. They follow a process of trial and error on innovations that are offered to users and proved somewhat uncertain to the benefits of the whole society. The European proposals on their territory are intended to be applicable regardless of the origin or the geographical location of the supplier, what requires a number of international initiatives and agreements that still seem distant.

C. *Perception of Privacy*

In the context of communicative functions, Jin Park [29] analysed three dimensions of the impact of digital literacy behaviours related to online privacy: a) familiarity with the technical aspects of the Internet, b) awareness of common and institutional aspects and c) understanding of the current privacy policy. The analysis showed a strong predictive capability of user's knowledge, but results were mixed when representing the interaction between the knowledge and experiences. There were limitations on the extensions of the knowledge and the action related to personalized information.

Moreover, these limitations were divided by sociodemographic characteristics such as age, gender, income and education. The study demonstrated the presence of a second-level digital divide in Internet privacy, apart from the level of access, both strongly influenced by temporal priority.

In this context, Fathi [30] distinguishes the following areas: perspective of security, authentication against impersonation, leakage resilient schemes, identity-based encryption for privacy, anonymity for privacy, private information retrieval for privacy and trust.

The lack of awareness about the immediate risks, the lack of rationality of users when providing personal data, the relevance of the temporal priority in literacy as well as the limitations between interaction of knowledge and action / experiences intimately related to memory, the liquid spheres from a technical perspective as from users behaviour one; lead to a worrying environment if bearing also in mind that Privacy Policies / Terms and Conditions

[5] “45% of Canadians willing to sell their digital data”, in: *CBC News Business*. 30 January 2014. URL [http://www.cbc.ca/news/business/45-of-canadians-willing-to-sell-their-digital-data-1.2517427]. Consult 4 February 2014.

[6] “More online Americans say they’ve experienced a personal data breach”. *Pew Research*. 14 April 2014. URL [http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach/]. Consult 14 April 2014.

[7] “Anonymity, Privacy, and Security Online”. *Pew Research*. 5 September 2013. URL [http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/]. Consult 14 April 2014.

[8] “Trading privacy for security in the online world”, in: *GRAND NCE*. 4 February 2014. URL [http://grand-nce.ca/newsandmedia/news-container/2014/trading-privacy-for-security-in-the-online-world]. Consult 4 February 2014.

are described as ambiguous and confused for a long time – 2005 [31] -, and unfortunately, still does as our research and others concluded. Moreover, it ought to be strength the relevance of language in the cognition process.

Therefore, in this liquid mobile environment where the data fluxes without frontiers, users deal with a great difficulty in applying their knowledge to actions; partly because of their own lack of awareness, partly because the information about Privacy Policies / Terms and Conditions as well as about technologies is ambiguous and confused. Temporal priority as a key factor also aggravates their ability.

The Architecture of Intimacy [32], the Architecture of Disclosure [33] and the Interface Design of Exposure [16], representing Facebook a primary example; strengthens this liquid environment, setting a design structure that encourages exposure and visibility to the detriment of protection and privacy.

D. Some Tendencies

The concept of 'continuous partial attention' proposed by Stone[9] explains how "being –always- on" affects the quality that users deliver to each of their tasks, under less "mind share". Focused on the identity, it refers how people think about their lives and priorities, which may be also affected. In this regard, the "Self" may lose the sense of conscious communication choice, since the media are always hold on in the background [18]. Hypothesis supported also by Starner[10], whose research to date suggests that our ability to multitask is not as great as we think, "when we multitask we do less well on more tasks".

Experience related to the concept of "mobile identity", introduced by Stald [34] and focused on youth, identity and mobile communications. It is mainly characterized by the "fluidity of identity" – constantly to be negotiated – based on four axis: 1) availability; 2) experience of presence where the social presence in public space is being invaded by mobile communication in progress; 3) personal log for activities, networking and communication of experiences, a role which has implications both for the relationship between the individual and the group, as for the emotional experience; and 4) learning of social norms.

These tendencies are closely related to the three technology revolutions according to Pew Research Centre 2014: 'Broadband, Mobile and Social', where contacts, location and synchronization between them seemed to be an increasingly valuable resource in the mobile ecosystem, as showed by recent business models strategies like the purchase of Instagram or WhatsApp by Facebook. Another tendency underlined by MIT in its technology reviews was that some mobile apps were starting to add anonymity to social networking. Specialized ads for mobile devices, mainly local, were also a growing trend.

In this environment, less than 40% of web traffic came from Human[11] where a new generation theory of the user interface stated that there ought not to be a user interface; information ought just to be around [35]. Moreover, the ability to add new features to mobile search has just begun, with proposals for the future as MindMeld, Expect Labs (2013), a personal assistant that infers the future user behaviour from the analysis of their conversations [1].

VI. OBJECTIVES AND METHODOLOGY

On the one hand, operative systems delimit programming environment, mobile platforms, user interface/experience and the norms to which apps developers, providers and distributors ought to stick to. On the other hand, environments – platforms - group the relation between the different actors through channel and services content distribution, configuring someway the apps stores. They articulate, apart from network operators, the operative system and the user interface/experience, the content management software/applications that serve as a control of user activity and the SDK, the software development kit.

Therefore, our research focused on the analyses of the interrelationships between the operative systems and its environment, the platforms and the applications choosing the privacy features configurations: Apple iOS (6.4.1), Android (2.3.5), Blackberry (5) and Windows Phone (7.5) with the platforms: Facebook, Twitter, LinkedIn, Google + and the applications Instagram, Vine, WhatsApp and Line.

Secondly, a comparison between the conditions and terms of privacy of the four platforms and the applications mentioned were carried out. Finally, the installation of all these platforms and applications were made both in Apple iOS and Android systems mainly as well as Blackberry and Windows Phone in order to appreciate similarities and differences in the process, in the results, in the interface design and in the action visibility.

Finally, some incipient conclusions from an exploratory focus group and a survey carried on in north Portugal will be added as a complement.

VII. DISCUSSION

A. Operative systems-environment, applications and platforms.

Main differences were found between the Apple iOS, Blackberry and Windows Phone system and the Google Android one. If establishing a comparison with solid and liquid spheres, the first group was observed as solid and the second one as liquid, whereas iOS Jailbreak or Amazon OS, for example, were placed in the middle of an ongoing process. From the date our analyses started until nowadays, an approximation and even dissolution of boundaries have been appreciated as a tendency. Closed ones have initiating a process of openness in its system and vice versa.

Generally, Apple iOS, Blackberry and Windows Phone made efforts trying to create 'Closed Environments' while Android followed the 'Open Source' market conception.

[9] "What is Continuous Partial Attention?" In: *Lindastone.net*. URL [http://lindastone.net/qa/continuous-partial-attention/]. Consult 8 February 2014.

[10] "Multiplexing versus multitasking". In: *The Technium*. URL [http://kk.org/thetechnium/2011/03/multiplexing-vs/]. Consult 11 February 2014.

[11] "Report: Bot traffic is up to 61.5% of all website traffic" by Igal Zeifman. In: *Incapsula.com*. URL [http://www.incapsula.com/blog/bot-traffic-report-2013.html]. Consult 24 January 2014.

Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018. URL [http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html]. Consult 1 April 2014.

This division in operative systems related to most of other aspects analysed due to the main root characteristic observed: whether it controlled more or less all functions and relationships between its hardware and the applications and platforms installed, as well as other services. As explained in the theoretical framework, Apple iOS relies on the tight control of its user database through the binomial OS-device, while Google Android does on an operative system linked to information aggregation services and its technologies of contextual and behavioural targeting.

In this sense, Apple iOS asked the user for permission before downloading any kind of app; whereas, in the rest, users had to confirm or not the access to them after downloading. This aspect was well exemplified when the Apple iOS asked for the control of all its registers – to be able to share content after, for example - as well as all the access of them to the hardware and to the mobile data.

Another example was that the user did not need to be connected to the app or platform (with it opened) to carry on actions through it. For instance, it was observed that the user was able to share the contents through different apps and platforms without having them officially opened. User data were defined in the operative system so it was able to be used by any app and its content sharing menu in Apple iOS and in WhatsApp for Windows Phone.

On the contrary, Android and Blackberry needed to have all the applications and platforms, specifically in the case of Facebook and Twitter, installed and opened for their options of content sharing menu were able to appear in others.

Deepening into concrete questions made to all systems, analysis started measuring whether they let modify all 'Privacy Settings' or not and at what level. Remembering previous main difference explained, Apple iOS controlled all of them, including those specific ones from applications and platforms, through its operative system by itself. Any time users want to alter the configuration of 'Security' or the 'Privacy Settings' of them, they had to change it through the operative system.

On the contrary, Android established its 'Privacy Settings' in direct link with the applications and the platforms so they had to be modified from the same (apps and platforms). Due to the fact that they may come from unknown and uncontrolled authors, Android provided a specific option to let or not let install them - "installation of applications from unknown authors" -. As an example, users were not able to register the applications and the platforms that employed the GPS and, then, alter its configuration in the operative system 'Settings'.

Then, the main aspects concerning the interrelationships between OS, its environment, apps and platforms will be listed and employed as epigraphs. They were the features or applications that employ personal information for different kind of purposes.

A.1. Privacy Settings

Elements analysed were: 'Location', 'Contacts', 'Calendar', 'Reminders', 'Photos', 'Bluetooth', 'Twitter', 'Facebook', 'Phone ID', 'Safari', 'Chrome', 'Internet Explorer', 'BB Browser', 'Opera Mini', 'Backup', 'Feedback-Data Sense' (when you signed the contract), 'Transmission of data application usage' (feedback application) and 'Sharing files between applications'.

The applications listed are the ones that established a direct link between the device and the user. For example, 'contacts' were high susceptible of offering great quantity of user data. A characteristic observed in Android was the fact that contacts did not have specific privacy settings in the operative system and neither in the applications and platforms. Windows Phone followed same patterns as Android when asking about if they allow modifying options of 'Privacy Settings' in the operative system. Blackberry was also similar to Android regarding 'Privacy Settings', being the only one that offered specifically the possibility of defining 'Firewall' protection – others might have it but they did not specify it -. Another unique feature of Blackberry was that the installation of the application had to be made through the computer connection.

Then, three tendencies were able to be described from 'Location' to 'Phone ID' elements: the first one was Apple iOS with all categories included in 'Settings' and with a list of authorized applications; also allowing access to Phone ID. Second one was Android with 'Location' and 'Bluetooth' in 'Settings', specific 'Google Calendar', 'Twitter' and 'Facebook' also in 'Settings' only if you had previously installed the application and allowed access to Phone ID.

Third one was Blackberry and Windows Phone with much in common as, for example, the inability to find the 'Phone ID' in 'Settings' as well as 'Contact', 'Calendar', 'Reminder' and 'Photos' and without a list of authorized applications. Blackberry had its 'Bluetooth' defined in 'Settings' while Windows Phone had 'Location' and 'Bluetooth' in 'Settings'. From this part of the analysis, two main different models of operative systems and market models, as mentioned in the beginning of the chapter, were able to be distinguished: Apple iOS, Blackberry and Windows Phone with a control over all applications and apps stores installed through its operative system and Google Android that allowed multiple apps stores being controlled by others.

Each operative system had a default browser installed (Safari, Chrome, BB Browser, Internet Explorer). These browser settings disposed of 'Private Browsing' and their own privacy, similar to a PC browser. In the case of Windows Phone, the option was the similar one 'do no track'. All of them supported 'Opera Mini' browser. Regarding browsing settings, a liquid convergence in the privacy settings were observed. That is to say, that all browsers had already found a common balance point to deal with privacy control.

Apple iOS and Windows Phone did not allow applications to have access to the common mobile files' system (except to the camera roll) while Android did it to part of the files. To end up with, Apple iOS, Blackberry and Windows Phone were able to be named as 'Controlled Developers' or 'Closed Environments'; while Android was able to be called 'Open Source'. Here, it was observed a clear delimitation of models (liquid-solid). However, the tendency is to open the closed ones and vice versa in order to share items with more security. As an example, the upcoming iOS 8 will share information between apps like Android already allows.

A.2. Features

In the following group, 'Java support', 'Flash support', 'Security', 'Social Media Integration', 'Social Gamming', 'Movie Store', 'Music Store', 'Book Store', 'Default Browser', 'Cloud Support', 'Cloud Messaging', 'Wireless Cloud Support', 'Parental Control', 'Remove Clear Data', 'Internet Wi-Fi', 'Internet 3G/4G', 'SIM/telephone' and 'Notifications System-Messages' were categories studied.

Only Android supported 'Flash', and with Blackberry 'Java'. It was someway a bit dangerous because of the ligations arose next to the hardware. In this regard, this aspect seemed to continue fixed, without variations.

Regarding 'Security', Android and Blackberry encrypted personal folder and Windows Phone had multilayer, secure boot, sandboxing and an encrypted sync. All of them presented 'Social Media Integration' while Apple iOS (Game Centre) and Windows Phone (Microsoft XBOX Live) its own 'Social Gamming' as well as 'Wireless Cloud Support'. There, it would be interesting to know whether it is an encrypted backup and if the connection is secure. The convergence point seemed that it is going to be the encrypted personal data and the wireless transmissions.

About Stores, nothing especially interesting might be mentioned. Most of them had their own applications, being Apple iOS: iTunes and iBooks, Android: nothing specific for music and Google Books, Blackberry: Rovi and Music Store RIM and Windows Phone: Zune, whereas the latter two might have also Amazon-Kindle. All offered as well 'Cloud Support & Messaging' being for Apple iOS: iCloud and iMessage, Android: Google Sync and Google Cloud Messaging, Blackberry: Third Party and Windows Phone: Sky Drive and Windows Messaging.

Only Apple iOS and Android systems offered 'Parental Control' and all of them allowed 'Remote Clear Data' except Android by default, but it could be offered by Samsung services. The reason might lay on the existence of different developers involved in the market and without an agreement between them. Internet Wi-Fi, 3G/4G, SIM/telephone, notification system and messages were placed in applications. That is to say, all applications and platforms had freedom to choose / set / select those features or not, they can be controlled by the user in the same.

A.3. Official Applications

The following ones have been studied: 'Maps, Google Play and Search, Gmail, Youtube, Pandora Radio, Apple iTunes, Cooliris, purchases in applications, Twitter, Yahoo Messenger, eBay Mobile, Amazon Mobile, LinkedIn, Flikr, Instagram, WhatsApp, Skype, Line, Viber, Foursquare, Pinterest and Facebook'. Main aspect to underline was 'Purchases in Applications' where Apple iOS controlled it as well as Windows Phone through MS Market/XBox Live and while Android and Blackberry did it through Google Wallet, Paypal or the application itself as in the case of Kindle.

A logical difference was that Apple iTunes only existed in Apple iOS. Android was the only one that allowed 'Google Play' and while Apple iOS had 'Cooliris', Android and Windows Phone had 'LiveShare' –Blackberry anything -. Flikr was not been found for Blackberry, neither Instagram for Windows Phone.

Despite all the differences, the convergence point seemed to be that all environments are going to have all the applications available in the future.

B. Privacy Terms and Conditions

Generally, it seemed that 'Privacy Terms and Conditions' were written to protect the company rather than the user since they were sometimes very ambiguous, opened to different interpretations and likely to expand its content to define future situations, the benefit of whom? Many aspects were analysed but, due to a matter of space, only those more linked to the delimitation of privacy were selected. One characteristic to underline was its volatility and constant change, therefore, its liquidity.

On the one hand: Facebook[12], Twitter[13], LinkedIn[14] and Google[15] (as Google +, our aim of study, followed the same terms and conditions of Google). On the other hand: Instagram[16], Vine[17], WhatsApp[18] and Line[19]. The first four were considered web services (although they had applications for mobile phones). The last 4 were App services (App called) because they required a previous installation of the application on the mobile device (even in the case the user only employed the web service), which makes sense as they are specifically designed to be used by a 'mobile phone behaviour'. Another difference was that the terms and conditions of the first group were more completed, developed and offered in more languages.

Three of the web services required a valid email to conclude the registration (only Google not), where Facebook required also date of birth and sex. Applications linked with calling functions required obviously your phone number and in the case of 'Line' a password was required for 'phone-book' multi-device function.

Regarding minimum age required to register: Twitter specified 13, LinkedIn 18 while Google did not specify it (leaving the requirement opened to the case of some additional products) neither Facebook, although this last one requested it to do the registration (13) and for some applications (18). A different approach was observed in the applications: "Instagram does not knowingly collect or solicit any information from anyone under the age of 13", Vine did not discriminate but indicated the service was for older than 13, "You affirm that you are either more than 16 years of age, or an emancipated minor...." WhatsApp and Line did not stipulate it but they had a child protection policy.

Differences were observed about who was the owner of personal information: Facebook did not particularize it although indicated that were the ones that you decided to share, neither Twitter pointing out the user allowed the company to use it. LinkedIn and Google designated that

[12] <https://www.facebook.com/about/privacy/; date: 11th December 2012. Facebook, 1601 Willow Road, Menlo Park, CA 94025 USA

[13] <https://twitter.com/privacy; date: 3rd July 2013. Address not specify on it, in the web: Twitter, Inc.1355 Market St, Suite 900. San Francisco, CA 94103

[14] <http://pt.linkedin.com/legal/privacy-policy; date: 12th September 2012. LinkedIn Corporation, 2029 Sierlin Court, Mountain View, CA 94043 USA.

[15] < http://www.google.com/intl/pt-PT/policiestica /privacy/; date: 24th June 2013 -analyzed two documents, 'Terms of Use and Privacy Policy'-. Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA.

[16] <http://instagram.com/about/legal/privacy; date: 19th January 2013.

[17] <https://vine.co/privacy/; date: 21st January 2013 –analyzed two documents, 'Terms of Service and Vine Privacy Policy'-. 1355 Market St., Suite 900 – San Francisco, CA 94103.

[18] <http://www.whatsapp.com/legal/; date: 7th July 2012. 3561 Homestead Road, #416, Santa Clara, CA 95010-5161

[19] <http://line.naver.jp/line_rules/en/; 1st April 2013.

the owner was the user but they also denoted that they were controlled by LinkedIn to protect users data and that the employment of Google did not confer the user any ownership over their services or accessed content. Instagram and Line did not itemize it, neither Vine that added "is a video sharing platform, so most of the information you provide us is information that you choose to be made public" and WhatsApp "...you retain your ownership rights in you 'Status Submissions', but you have to have the rights in the first place." This was a clear example of the ambiguity found in the analysed terms and conditions.

They all collected data from its use and from other sites or applications except WhatsApp and Line, it might be because they lacked of external partners. Also they all utilized cookies or similar technologies and gathered specific metadata to catch other information. Only Facebook and Twitter particularized the option of 'do not track' – tracing - although all indicate that they might prevent the browser use cookies.

They all offered the possibility to alter the information, disable, suspend or eliminate totally the account but, in the case of Google, it was the only one that did not refer specifically to the act of closing an account and it also did not ensure to be able to delete data account. Twitter and Line were the only ones that did not concrete where information was stored, what might be interpreted as this aspect will depend on each country law system. Concerning a specific data protection policy, once more, they were ambiguous or they did not describe a detailed one. They simply stated they will do the best they can and recommended the user to behave properly and help at this point.

One difference between the first group (called mainly sites, Facebook, Twitter, LinkedIn and Google) and the second one (applications Instagram, Vine, WhatsApp and Line) was that, regarding the possible circle of public to share the content with, they were more or less restricted to contacts saved on the mobile phone account. It meant that when answering to the question of allowing other sites, applications, platforms, services or users to access the account, the range was wider in the first group.

The majority of them detailed, or simply did not specify leaving this aspect opened, that users information was shared with other platforms, sites, applications, services or other users in the name of different purposes: personalized content, improve services, inform friends, make suggestions, etc. Here it had to be stress the fact that they would disclose information by law request or to protect their services, leaving this aspect again opened to various interpretations.

All of them had the concern to create targeted or custom ads, where LinkedIn had a specific part to describe how to deal with it. All first group and WhatsApp offered concretely the option of blocking ads. Facebook, LinkedIn and Google were adhered to some kind of regulatory authority. Also all of them, except Line, indicated the terms of sale of the service or the company as well as the updates of the 'Terms and Privacy Policy'. In practice, users had to be aware of them by their own as not always they would be informed through a direct contact from the company.

Another difference between groups was that none applications specify a policy targeted to children while only Twitter did it. Neither Google nor any applications detailed if they fulfilled 'Safe Harbour[20]' and 'TRUSTe[21]' rules or 'Shine the Light' Law of California[22] (direct marketing). Facebook and LinkedIn stated they did it and Twitter just mentioned the first one.

The interest for collection personal information and its sharing through social media is so widespread and relevant that all environments and platforms accepted being opened to others in order to obtain as much data as possible, generating a liquidity state for the data flux.

C. *Exploratory Focus Group and Survey*

C.1. Exploratory Focus Group[23]

Sociability, coordination and its maintenance were outstanding while issues related to personal and professional life were also considered very important, in some cases essential. There, it ought to be remembered the characteristics of fluidity of identity as well as the cellular and nomadic intimacy, constantly to be negotiated.

The issue of privacy appeared in two ways: in the level of content/data and in the level of interaction contexts. There was a concerned in the perception of privacy when producing a mobile phone appropriation by others. They stated reluctance to lend it beyond a momentary use to call and the ignorance – no control - over the audience. There was a notion of existence some risk of exposure/personal aspects to last in time online, but the practices seemed to be unconcerned. Participants tended to consider that the data was always private, but in some cases (images) did not contradict the possibility of share/publish them.

This observation matched previous studies mentioned: users concerns were too remote to influence their decisions - although they took some steps to prevent - compared with the immediate and tangible benefits of that same sharing – emotion involved and, even in the case of Canada, to sell personal data for a good prize -. Moreover, the risks were not so evident because they continued to act as if they had privacy. These attitudes remind some kind of lack of rationality described in the theoretical frame.

The group discussion highlighted the difference between two types of risk about the privacy of content/information: the data stored/fixed in a device (computer/phone's) and the data that became accessible by third parties at any time and place online – contextual integrity - . The concern of disseminating pictures of them had to do with the embarrassing situations and aesthetics of the images. Its publication in open or closed circles was produced by the "good common sense". They showed high tolerance to invasion/harassment commercial use of not allowed personal data.

At this point, they showed an initial awareness of the different sources to collect their personal data. However, the possibilities are wider as it was described in the theoretical frame concerning profile and digital identity. Therefore, the required knowledge ought to be transmitted in this area.

To end up, some general appreciations like the anxiety cause due to the fact of "having to be always available", to

[20] <http://export.gov/safeharbor/; consult 28th September 2013

[21] <http://www.truste.com/; consult 28th September 2013

[22] <http://en.wikipedia.org/wiki/California_Shine_the_Light_law; consult 28th September 2013

[23] Covilhã, Portugal, July 2013th. 3 males and 3 females, ages: 19, 2*20, 2*21, 23.

answer depending on who is calling, the reluctance to speak in public near unknown people, not to constrain sociability or interrupt conversations by mobile phone and the strategy to minimize risk of nuisance (silence mode/vibrator) are pointed.

C.2. Exploratory Survey[24]

Basic function, such as 'do calls' and 'send and receive text messages' were those that respondents privilege in their use, several times a day. In a second group, those respondents who used their device to, also several times a day, 'visit sites, browse the Internet, searching information' and still 'visit social networking sites'. 71% used the phone for taking photos or videos between one and three times per week. Closeness with people was crucial to lend or borrow mobiles. There exists a strong sense of property "it's my phone".

68% checked if the application offered "application permission" but 61% did not read those "permissions" before installing, being 32% who did. 55% did not allow apps to access the lists of contacts or information. Half took, therefore, some steps to prevent the synchronization of data.

Half might live without mobile phones, 32% would felt their lack and 18% considered that they did not have such a powerful role in their lives. Its use was strong circumstantial, very dependent on circumstances, since there were no general rules self-stipulated by the actors in relation to the different life situations, they dealt different behaviours according to the context. 63,5% agreed "I feel uncomfortable when I have to make a call and there are strangers around me", while "agree" and "totally agree", added 94,6%.

This strong circumstantial use highlighted relevant characteristics described in the theoretical frame: the fluidity of identity, the cellular and nomadic intimacy and the relevance of temporal priority in the digital literacy.

VIII. CONCLUSIONS

Regarding operative systems on smartphones, two main models were observed, iOS 'Closed Environment' controlling everything around the smartphone: Equipment, SDK, Apps, Market (App Store) as well as users and Android 'Open Source' allowing the freewill behaviour. Following this concept and concerning Privacy, iOS controlled the user data from applications and platforms while Android could or could not, depending of what allowed in each application and platform as well as their relationship with Google as an intermediate.

One important difference between them was that, after accepting both an installation, only through iOS user could alter the 'Privacy Configurations' related to its environment while in Android users had to reinstall if they did not agree with the whole package formerly accepted. Moreover, iOS offered the possibility to alter, for example GPS or contacts, in each application or platform whereas in Android the user could accept it or not for all of them.

In terms of security characteristics, the tendency seemed to be for all the environments to get closer, less liquid. That is to say, to adapt to the requirements of user privacy concerns, as it is going to be explained.

The lack of control about how and who accessed to the data and contents published, according to the literature review and the exploratory studies, was what users aware and worried about but they also seemed not to take many actions to prevent, except localization and the access to the list of contacts when installing or setting applications. To avoid synchronization and to use a new mail account to register could be partial solutions for these concerns.

As one and main example of the volatility and ambiguity of the 'Terms and Conditions' analysed, Google cannot guarantee full delete of users information account and none of them specify a data protection policy, leaving this question mainly to user's good sense, who had to be aware of the possible updates of the 'Terms and Conditions'. At this point, Google is right now working on a proposal for the 'Right to be Forgotten'.

The liquidity observed in the society and in the mobile environment as well as between the public and private spheres, can also be applied to the operative systems. iOS, Blackberry and Windows Phone started being a solid sphere (lack of external versions in its market) that are experiencing a process of liquidity (allowing access to others despite keeping a tight control). Meanwhile, Android begun totally liquid (open) and is increasingly becoming more solid (due to its concerns about Privacy, for example, Amazon getting closed). This tendency could lead to reach a convergence meeting point where both brands / developers and users would have the control of Privacy. Both spheres / operative systems and its development are dealing with a process of liquidity.

Bearing in mind such defining features of smartphones like instantaneity and ubiquity; concerning literacy, the continuous partial attention and its relation with memory; the lack of rationality in some attitudes and performances; the limitations on the extension between knowledge and action; the strong circumstantial pattern behaviour; the volatility and ambiguity of the 'Terms and Conditions', adding the liquidity and mobility of our society and technology itself; the users deal with liquid spheres where the constant data flux escapes from a clear awareness of it and a notion of the risks involved in deep.

Therefore, the users manage a constant negotiation of circumstances based on the evaluation of each scenario framed by the ambiguity and the immediacy, which also determines the reflectivity (required time to analyse) as well as the perception of the risk involved in every action. Moreover, the possibility of receiving stimuli of all types constantly influences how to establish the priority level properly as well as how to protect their privacy at the different layers and stages according to their possibilities.

REFERENCES

[1] J. M. Aguado, C. Feijóo, I.J. Martínez (cords.), *La comunicación móvil. Hacia un Nuevo ecosistema digital,* Barcelona: Gedisa, 2013, p. 18, p. 30, p. 31, p. 308, p. 309, pp. 318-320, p. 41.

[2] Z. Bauman, *In Search of Politics,* Stanford University Press, 1999 / *Em busca da política*. Rio de Janeiro: Zahar, 2008.

[3] Z. Bauman, *Vida para consumo. A transformação das pessoas em mercadoria,* Rio de Janeiro: Zahar, 2000, p. 71.

[4] B. Wellman, "Physical Place and Cyberplace: The Rise of Personalized Networking". *International Journal of Urban and Regional*

[24] Portugal: from 15th July until 21st August 2013, online. It had 74 answers and largest number of respondents was in the age group between 30 and 45 years old – nobody less than 18 and more than 65 -; 56,8% women and 43,2% men. 73% employed, being 85,7% women and 81,2% men with higher education. 67,7% had a smartphone and 31 % not.

Research, 2001, 25, pp. 227–52. http://dx.doi.org/10.1111/1468-2427.00309

[5] J. Katz, M. Castells (eds), *Handbook of Mobile Communication Studies,* Cambridge: MIT Press, 2008, p. 49. http://dx.doi.org/10.7551/mitpress/9780262113120.001.0001

[6] J.E. Katz, M. Aakhus (eds), *Perpetual Contact. Mobile Communication, Private Talk, Public Performance*, Cambridge: Cambridge University Press, 2002. http://dx.doi.org/10.1017/CBO9780511489471

[7] A. Fidalgo, A. Serrano Tellería, J.R. Carvalheiro, J. Canavilhãs, J.C. Correia JC, “Human Being as a Communication Portal: The construction of the Profile on Mobile Phones”, *Revista Latina de Comunicación Social*, 2013, 68. http://dx.doi.org/10.4185/RLCS-2013-989en

[8] K. Kawamoto, *Media and Society In the Digital Age*, New York: University of Washington, 2003, p. 33.

[9] Z. Bauman Z, *Liquid Life*, Cambridge: Polity, 2005.

[10] S. Isabella, “Mobile Phone: Users Practices and Innovations Between Public and Private Sphere”. In *COST 298 Conference. Participation in the Broadband Society*, 2009, p. 7.

[11] L. Fortunati, "The Mobile Phone: Towards New Categories and Social Relations". In *Information, Communication, and Society*, 2002, pp. 514-528.

[12] A. Fidalgo, “Conectados e tutelados. Uma revisitação tecnológica da esfera pública”, in *Public Sphere Reconsidered: Theories and Practices*, Beira Interior University: LabCom, 2011, p. 68, pp.68-70.

[13] H. Geser, “Is the cell phone undermining the social order?”, in *Thumb Culture*, Bielefeld: Transcript Verlag, 2005, p. 25.

[14] T. Ahonen, “Mobile as 7th of the Mass Media. Cellphone, Cameraphone, IPhone, Smartphone”, in *Futuretext*, 2008.

[15] J. E. Katz, “Mainstreamed Mobiles in Daily Life: Perspectives and Prospects”, in Katz, Castells (eds.), *Handbook of Mobile Communication Studies*, Cambridge: MIT Press, 2008. http://dx.doi.org/10.7551/mitpress/9780262113120.003.0032

[16] A. Serrano Tellería, “The Construction of Profiles on Mobile Phones. Public and Private Spheres”, in *DESIGNA 2013: INTERFACE International Congress*, 21 & 22 November, Beira Interior University: LabCom, 2014.

[17] M. Mazmanian, *Some thoughts on blackberries*, Memo, 2005.

[18] S. Turkle, “Always-On / Always-on-You”: The Tethered Self”, in Katz, Castells (eds), *Handbook of Mobile Communication Studies*, Cambridge: MIT Press, 2008, p. 128, p. 129. http://dx.doi.org/10.7551/mitpress/9780262113120.003.0010

[19] R. Sennett, *The Fall of Public Man*, New York: Penguin Books, 2002, p.36.

[20] J. Meyrowitz, *No Sense of Place: The Impact of Electronic Media on Social Behavior*, New York: Oxford University, 1985.

[21] E. Goffman, *The presentation of Self in everyday life*, New York: Garden City, 1959 / *A Apresentação do Eu na Vida de Todos os Dias*, Lisboa: Relógio d’Água, 1993.

[22] D. McQuail, *Mass Communication Theory*, London: Sage, 2006.

[23] A. Castellet, *El ecosistema del contenido móvil: actores, líneas de evolución y factores de disrupción*, Ph.D dissertation, Spain: Murcia University, 2012.

[24] J. McDermott, “IPhone owners consume more entertainment than Android”, in *Advertising Age, adage.com*, 25 March 2013.

[25] S. B. Wicker, “The Loss of Location Privacy in the Cellular Age”. Communications of the ACM, 2012, 55(8), pp. 60-68. http://dx.doi.org/10.1145/2240236.2240255

[26] A. Cerra, C. James, *Identity Shift,* Indianapolis: John Wiley & Sons, 2012.

[27] D. Potoglou, D. Patil, C. Gijón-Tascón, J. Palacios, C. Feijóo, “The value of personal information online: results from three stated preference discrete choice experiments in the UK”. *European Conference on Information Systems, ECIS 2013*, Utrecht, Netherlands, 2013, pp. 1-12.

[28] H. Nissembaum, *Privacy in context. Technology, policy and the integrity of social life*, Stanford: Stanford University Press, 2010.

[29] J. Jin Park, “Digital Literacy and Privacy Behaviors Online”, in *Communication Research*: Sage, 23 August 2011.

[30] H. Fathi, “Security and Privacy Challenges in Globalized Wireless Communications”, in: Prasad et al. (eds.) *Globalization of Mobile and Wireless Communications: Today and in 2020, Signals and Communication Technology,* Springer, 2011. http://dx.doi.org/10.1007/978-94-007-0107-6_7

[31] J. Fernback, Z. Papacharissi, “Online privacy as legal safeguard: the relationship among consumer, online portal and privacy policies”, in *New Media and Society*, 2007, 9, 715. http://dx.doi.org/10.1177/1461444807080336

[32] S. Turkle, *Alone Together: Why we expext more from technology and less from each other*, New York: Basic Books, 2011.

[33] J. Marichal, *Facebook Democracy. The Architecture of Disclosure and the Threat to Public Life*, United Kingdom: Ashgate, 2012.

[34] G. Stald, “Mobile Identity: Youth, Identity, and Mobile Communication Media." In: Buckingham D. *Youth, Identity, and Digital Media.* The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning, Cambridge, MA: The MIT Press, 2008, pp. 143–164.

[35] J. Manyika, “The impact of disruptive technology. A conversation with Eric Schmift”, in: *McKinsey & Company, mckinsey.com*, 2013.

AUTHORS

A. Serrano Tellería. Ph.D Assistant Professor. Posdoc, Ph.D candidates (5) coordinator of the European FEDER project 'Public and Private in Mobile Communications' in LabCom, Beira Interior University, Portugal (April 2013 - 2015). Lecturer of Cyberculture (2013-14). Ph.D. (2010) and Bachelor in Journalism (2002) by the University of The Basque Country. Extraordinary Ph.D Award (2012). First cycle of English Translation and Interpretation (2000). Management of European projects and International Cooperation ones in Documenta (2012-13). Responsible of the Communication Department in the Territorial Development Agency "Campoo Los Valles" (2011). Master in Innovation Management (Full grant, 2010-11). Visiting researcher at the School of Communication in Federal University of Salvador de Bahia, Brazil (Grant of the Spanish Ministry of Science and Innovation, 2009). Cultural Management (2005). Master in Theatre and Performing Arts (2004-05). Theatre teacher (2003-04). Online journalist in *Elcorreo.com*, Vocento (2002-03). Email: anaserranotelleria@gmail.com.

M. Oliveira. Ms.C Computer Scientist. Master's in Computer Engineering from the University of Beira Interior in 2009. He has been performing duties as senior technician in the areas of web development and administration of systems in the Online Communication Laboratory (LabCom) at Beira Interior University since 2005. Email: marco.oliveira@labcom.ubi.pt.

This work was supported in part by the European Union and MAIS CENTRO (Portuguese Government). This article is result of the European FEDER project ‘Public and Private in Mobile Communications’, Online Communication Laboratory (LabCom), Faculty of Arts and Letters, Beira Interior University, Portugal. Ref: CENTRO-07ST24-FEDER-002017, April 2013 - 2015.

Submitted 28 July 2014. Published as resubmitted by the authors on September 24, 2014.

ANNEX. FEEDBACK FROM ITS INSTALLATION

Aspects related to ‘Privacy’ and tools concerning definition of personal image and ‘Public and Private’ Spheres were analyzed. Tests had been carried on four mobile phones with different operative systems. It should be underlined that each application is continuously being updated so the different aspects analyzed may be altered after this observation and comparative study (April 2014).

A. *Facebook*

Focusing in ‘Privacy Settings’, Android asked users to allow who could search your ‘chronology’ by name. Blackberry and Windows phone sent you with a direct link to Facebook webpage to read there ‘Privacy Terms and Conditions’; in this last case, there were no options to ‘privacy settings’ in the profile, the user could only set ‘localization’. There were more options about ‘push notifications’ in iOS than in the rest of the operative systems.

B. *Twitter (4.3.0.8 for Blackberry, 5.11 for iOS)*

In its webpage, there were headlands for ‘Security’ and ‘Privacy’ that were not found in the mobile application.

iOS asked to refresh ‘user’ settings’, ‘localization’ and questions about different types of ‘permissions’. Only ‘login verification’ was placed in the same, iOS controlled the rest through its operative system. Android and Blackberry requested access to: Location, contacts, accounts, access to the memory card, internet access, location, system tools, network, synchronization, informal personal contact data, account authenticator, manage lists of accounts, control the vibrator, discover accounts known and Google services.

Blackberry asked about content access, Twitter license contracts and in ‘settings’: refresh, Blackberry messenger, possibility to add GPS to the tweet, profile edition and assistance. Interface design of Windows Phone was similar to web one but it only offered the option of allowing GPS, new followers, instant messages or if the user is mentioned in a tweet. To ‘log out’ the user had to remove data account.

C. *LinkedIn (6.2 for iOS)*

Installing the application, iOS system asked if the user would like to receive ‘push notifications” to alter sound, icons and contacts while Android one ‘count and configuration’, ‘privacy settings’ and ‘application permissions’: ID Phone, system tools, personal information, manage the accounts list, USB storage, full access to Internet, hide/discover accounts, control of vibrator by hardware, system tools-sync, Internet communication.

Windows Phone only offered ‘settings’ and ‘notifications’ whereas Android ‘settings: Sync, notifications, push and about ‘Privacy Policy: Access to website and Copyright Information’. iOS app shared similar configuration, presenting a difference about ‘feedback’ when the user receives messages about the application.

D. *Google (+) (Android, 4.5.1 for iOS, 2.11.166 for Blackberry)*

Official applications neither for Windows Phone nor for Blackberry were found. iOS asked permission to access photos and create a security copy of them while Android did to: control hardware (audio, photo and video), and exact location, communication, system tools, telephone calls, personal data, accounts and storage. Other optional ones were: automatically update when connecting to Wi-Fi, create security copies of the photos and "allow Google to provide suggestions based on the people you communicate with most often on this phone".

E. *WhatsApp (2.11.4 for iOS)*

Android asked access for ‘Personal Information, Hardware Control, User Location, total access to Internet, services that costs money, calls, read status and Phone ID and to change system definitions’. Permission to access your contacts was also requested in Blackberry.

F. *Instagram (4.1.4 for iOS, 4.1.2 for Android)*

Questions about the installation in Android were: ‘Hardware control, recording audio, taking pictures and recording videos, system, personal information, location, storage, network'. iOS version just required access concerning photos. No versions found for Windows Phone and Blackberry.

G. *Vine*

iOS version asked the user if older than 17 years old, to access Twitter accounts, localization, push notifications and contacts while redirecting to the web about ‘Privacy Policies’. No findings for Android, Windows Mobile and Blackberry.

H. *Line (3.9.0 for iOS, 3.9.1 for Android, 1.9.15 for Blackberry)*

iOS asked about: push notifications, email, telephone, Facebook account and authorized apps while Android requested more permission: ‘Hardware control, localization, services implying payment, communication network, system utilities, telephone calls, personal data, messages and storage'. Blackberry just asked about contacts.