Privacy Perception when Using Smartphone Applications

Mobile Networks and Applications manuscript No.
(will be inserted by the editor)

Privacy Perception when using Smartphone Applications

Marco Furini · Silvia Mirri · Manuela Montangero · Catia Prandi

Received: date / Accepted: date

Abstract Our smartphone is full of applications and data that analytically organize, facilitate and describe our lives. We install applications for the most varied reasons, to inform us, to have fun, for work, for necessity, but, unfortunately, we often install them without reading the terms and conditions of use. The result is that our privacy is increasingly at risk. Considering this scenario, in this paper, we analyze the user's perception towards privacy while using smartphone applications. In particular, we formulate two different hypotheses: 1) the perception of privacy is influenced by the knowledge of the data used by the installed applications; 2) applications access to much more data than they need. The study is based on two questionnaires (within-subject experiments with 200 volunteers) and on the lists of installed apps (30 volunteers). Results show a widespread abuse of data related to location, personal contacts, camera, Wi-Fi network list, running apps list, and vibration. An in-depth analysis shows that some features are more relevant to certain groups of users (e.g., adults are mainly worried about contacts and Wi-Fi connection lists; iOS users are sensitive to smartphone vibration; female participants are worried about possible misuse of the smartphone camera).

M. Furini
Dipartimento di Comunicazione ed Economia
Università di Modena and Reggio Emilia, Viale Allegri 9, Reggio Emilia, 42121, Italy,
E-mail: marco.furini@unimore.it

S. Mirri and C. Prandi
Dipartimento di Informatica - Scienza e Ingegneria
Università di Bologna, Mura Anteo Zamboni 7, Bologna, 40126, Italy,
E-mail: {silvia.mirri,catia.prandi2}@unibo.it

M. Montangero
Dipartimento di Fisica, Informatica e Matematica
Università di Modena and Reggio Emilia, Via Campi XX, Modena, 41125, Italy,
E-mail: manuela.montangero@unimore.it

1 Introduction

It has been a long time since the concept of privacy appeared in 1890 [1]. In an article on *Harvard law Review*, Brandeis and Warren mentioned, for the first time, the right to privacy, the right to be let alone, the relevance of the intangible and the need to take legal action to "protect the person and the individual" from the ever increasing popularity of "recent inventions and business methods" (referring to the advent of photography and the widespread diffusion of newspapers) [1]. In short, the right to privacy was defined as the right of each individual to protect the psychological integrity by exercising control over information that reflected and influenced the personality of the individual. Today, the Cambridge dictionary defines privacy as "someone's right to keep their personal matters and relationships secret" as well as "the right to be alone and do things without other people seeing or hearing you"[1]. What emerges from such definitions is that privacy is an untouchable right, protecting both tangible and intangible properties. In essence, privacy can be defined as the ability of people to control when, how and to what extent their personal information is accessed [2]. Unfortunately, different studies and real-life examples show that privacy is becoming an "illusory" concept [3]: on the one side, it is quite easy to gather, store and share personal information and, on the other side, it is almost impossible to control and protect all the personal information that others might have access to. The Cambridge Analytica case [4] is one of the most popular example that brought privacy to headlines and highlighted how difficult it is to protect our privacy in the social network era.

In this paper, we focus on the mobile ecosystem and on the use of the smartphone in our daily life. The smartphone has become the hub of our life: it is our agenda, our financial promoter, our source of information, the door to an infinite world of entertainment, the thread that links us to our social life, the tool that connects us to our work 24H, the doctor who controls us when we do sports, the professor who teaches us something, the device that helps us to bypass some kind of disabilities, the second-screen we use while watching TV [5–12]. It contains very personal and sensitive data such as personal contacts, messages and locations, but also biometric data such as heart beat, blood oxygenation, face ID and fingerprints [13–15].

In this environment, are we able to protect our privacy? Are we able to control when, how and to what extent our personal information is accessed? No, our privacy is at risk [14,16–18] and the mobile ecosystem seems to be the most threatening scenario for privacy [19–21]. A well-known example of privacy violation was the *Flashlight* application [14]: the application simply had to turn on the flashlight of the smartphone, but an in-depth analysis found out that the application accessed to the phone number, to the device ID, to the precise user's location. Furthermore, it could control the hardware and the system tools, it could change the system configuration and the display settings. However, before blaming the applications, it is worth remembering that users

[1] https://dictionary.cambridge.org/dictionary/english/privacy

choose, install and accept the terms of use of the applications. Roughly, users allow applications to access their data; users do not read terms of use and ignore the permissions they give to the applications [22]. In the literature, different studies focused on this users' behavior and they highlighted various reasons (e.g., lack of motivation, useless effort, waste of time) that lead users to press the "agree" button without double thoughts [23–25]. The discrepancy between user's behavior and users' privacy is called *privacy paradox* and is a well-studied phenomenon in online profiling systems and social media contexts [26]. Our goal is to understand the privacy perception and the user behavior while using the smartphone device. We formulate two hypotheses:

- **H1**: users underestimate the importance of the data stored in the smartphone and this scarce knowledge affects their perception towards privacy;
- **H2**: users are not concerned of when, how and to what extent their personal information are accessed: they install applications without investigating which data will be retrieved and if these are really necessary to the application functioning.

To investigate H1, we developed a questionnaire related to different types of sensitive data (i.e., phone book contacts, the list of Wi-Fi connections, the list of running applications, the smartphone ID, the data of the multimedia storage, the type and the name of the cellular network provider, the SMS) and to different device sensors (i.e., microphone, vibration, camera, GPS). Then, we asked for volunteers to participate in the experiment and we involved 200 participants. The procedure worked as follows: 1) we asked volunteers to fill the questionnaire; 2) we provided participants with some examples of abuses for each type of data/sensor; 3) we asked volunteers to fill the same questionnaire of phase 1. By comparing the results obtained in phase 1 and 3, we have insights about the importance of the introduced knowledge. To anticipate here some results, among women, concern grows when possible abuses are discovered through microphone (+45%) and camera (+42%), whereas iOS users increase their concerns when the misuse is related to the list of running apps (+66%).

To investigate H2, we asked 30 volunteers to provide us the list of all the apps they have installed on their smartphones. Then, for each application, we checked the permissions that were requested to the user (i.e., we manually analyzed more than 800 apps to verify the requested permissions). Finally, we have identified the abuses (access to data not necessary for the application to work) and the types of data/sensors that are most at risk of privacy. The obtained results confirmed H2: a widespread abuse, especially for what regards contacts, camera, Wi-Fi network list, running apps list, and vibration. If concerned, users would not have installed many such applications.

In general, results highlight the users' ignorance towards privacy in the mobile ecosystem: people are not worried about privacy because they are unaware of the possible consequences and when they become aware of possible abuses, their concerns grow. Therefore, to protect privacy, it is necessary to improve the users' knowledge. Unfortunately, this is not an easy task, for two main reasons: (i) users ignore permissions for various reasons and they press

"agree" without even realizing the possible misuse of the data they are unleashing [23]; (ii) people have different habits and perception towards privacy. For example, *Alice* might consider her contact list very important, but not her location. Conversely, *Bob* might give importance to his location and not to his contacts. Our study might be considered the first step towards a more secure mobile ecosystem as it identifies features that are relevant to specific types of users [27]. For instance, adults are worried about phonebook contacts and Wi-Fi connection list, iOS users are sensitive to the smartphone vibration, female participants are worried about possible misuse of the smartphone camera. By combining features and types of users, it might be possible to design mechanisms and methodologies to improve the clarity and the transparency of authorization requests, to force app developers, OS and phone producers to provide warnings tailored to users.

The remainder of the paper is organized as follows: Section 2 presents recent studies focused on privacy in the mobile ecosystem; Section 3 describes methods, data and results of the performed analysis; Section 4 analyzes the users' behavior and in Section 5 we draw our conclusions.

2 Literature Review

In literature, different studies focused on technological solutions to preserve privacy in the mobile ecosystem [28–30], but since our focus is different, in the following we review studies that focused on privacy perception and/or users' behavior in the mobile environment. Shklovski et al. [14] focused on Android users and used a questionnaire to investigate the relationship between privacy and mobile users. Results showed that users felt their personal space violated when they are confronted with the behaviors of the apps installed on their phones. Khalid et al. [31] focused on privacy perception and analyzed user-reviews available on the app stores. Results showed that privacy is the most negatively-impacting complaint. Aditya et al. [21] focused on privacy threats and compared the mobile environment against the classic ones. Results highlighted that privacy threats within the mobile environment are different and more dangerous than in prior systems. Baig et al. [32] focused on mobile healthcare applications and found out critical issues and challenges related to security and privacy of data. Balebako et al. [20] focused on game applications and conducted a lab study with 19 participants to investigate their existing understanding of potential privacy leakages while using two smartphone game applications. Results showed that 13 out of 19 participants did not know that data would be shared for the purpose of advertising. Alenzei and Almomani [33] focused on Android OS and analyzed the 71 most rated educational apps and they classified the requested permissions into four categories (i.e., from normal to dangerous) in order to improve the users' awareness towards possible misuse of personal data.

A few studies analyzed the user's behavior regarding application permissions, proposing strategies to increase awareness. In [24], the authors present

an approach to assist users in understanding and deciding upon apps privacy implications, through the implementation of a mobile application, called Aware. Such an application provides users with the summary of the applications installed on the smartphone, the resources they access, and what are the motivations for that. Moreover, the app is capable of nudging (in the form of notifications) the user when certain sensitive data are accessed. A similar approach has been investigated by Hazim et al. [34]. The authors evaluated the benefits of giving users an app permission manager and of sending them nudges intended to raise their awareness of the data collected by their apps. Through a test applied to 23 participants, they showed that nudges cause users to more effectively control their privacy. Although interesting, it is to note that the results are based on a limited set of data (23 participants and 18 days of monitoring). Liu et al. [35] proposed and evaluated a "Personalized Privacy Assistant" able to assist users in permission settings. Users appreciated the assistant, but participants only changed 5.1% of the settings previously adopted. Our study deepens the privacy perception study (i.e., in addition to the generic perception, our goal is to investigate privacy perception towards personal contacts, smartphone camera, Wi-Fi networks list, running apps list, and vibration) and the user's behavior study (i.e., through the analysis of the apps actually installed on the users' smartphones)

3 Privacy Perception Analysis

3.1 Methodology

To understand privacy perception (H1), we developed a questionnaire based on a within-subject approach, where the controlled variable is the knowledge about possible misuse of user's data. The first part of the questionnaire establishes the initial perception towards privacy: a simple question about privacy *"Rate the importance you give to your privacy when using a smartphone"* with alternative answers ("high", "moderate", "some", "none", and "no idea") and 7 specific questions concerning *personal contacts, multimedia contents, Wi-Fi connections, microphone, camera, running apps*, and *vibration*. The second part of the questionnaire introduces the controlled variable, i.e. knowledge on possible problems users might incur in by sharing specific kind of data (e.g., access to microphone allows an App to record conversations going on around the phone) and repeats the same questions of the first part.

3.2 Participants

We asked for volunteers participations over our universities' platforms and we received collaboration by 200 volunteers: 55% female and 45% male, 70% young (below 30 years of age) and 30% adult (above 30 years), 66% with Android phone and 32% with iOS phone.

Table 1: Overall Privacy Perception

		High	Moderate	Some	None	No Idea
All	Before	30%	51%	9%	0%	10%
	After	82%	16%	1%	0%	1%
Male	Before	38%	45%	8%	0%	9%
	After	77%	21%	1%	0%	1%
Female	Before	23%	55%	11%	0%	11%
	After	87%	12%	0%	0%	1%
Android	Before	33%	49%	10%	0%	9%
	After	81%	17%	1%	0%	2%
iOS	Before	24%	59%	7%	0%	9%
	After	87%	13%	0%	0%	0%
Young Adults	Before	27%	43%	8%	0%	10%
	After	82%	13%	1%	0%	1%
Adults	Before	37%	39%	14%	0%	10%
	After	82%	14%	0%	0%	2%

3.3 Results

In the following, we present the results obtained from analyzing the answers to the questionnaire. In addition to the obtained results, we show the p value of the t.test (alpha=0.05) that checks whether results are statistically significant or not.

Overall Perception: *"Rate the importance you give to your privacy when using a smartphone"*. Table 1 shows the importance given to privacy by participants. Initially, the majority of the participants selected "moderate" (51%). Looking at the different categories, the "moderate" answer was the most selected one by male users (45%), female users (55%), Android users (49%), iOS users (59%), young-adults (43%) and adults (39%). Then, we show participants some examples of what malicious apps can do and the perception completely changed and the most selected option was "high": all users (82%), male users (77%), female users (87%), Android users (81%), iOS users (87%), Young adults (82%) and adults (82%). Results are statistically significant as $p < 0.0001$ and confirm **H1**: the introduced variable (i.e., the knowledge about possible misuse of smartphone data) affected the participants' answers.

Contacts. *"Rate the importance you give to your contacts list when using a smartphone"*. The extra knowledge given before the second part of the test is: *malicious apps might get and sell your contacts list.* The "high" option moved from 30% to 82% ($p = 0.0063$). A deeper analysis shows that female participants were more worried than males and also that extra knowledge affected both groups in a similar way: +64% ($p = 0.008$) for females and +39% ($p = 0.241$) for males. However, it is to note that results for male participants were not statistically significant. With respect to the other categories: Android (+58%, $p = 0.022$), iOS (+63%, $p = 0.153$), young adults (+55%, $p = 0.019$)), adults (+45%, $p = 0.138$)).

Microphone. *"Rate the importance you give to the microphone device when using a smartphone"*. The extra knowledge given before the second part

is: *malicious apps might turn your microphone on and record everything you say and hear.* On average, the "high" option moved from 46% to 80% ($p < 0.0001$). In details, male users (+20%, $p = 0.021$), female users (+45%, $p < 0.0001$), Android users (+30%, $p < 0.0001$), iOS users (+43%, $p < .0004$), young adults (+34%, $p = 0.002$) and adults (+31%, $p < 0.0001$).

Wi-Fi connections. *"Rate the importance you give to the Wi-Fi connections list when using a smartphone"*. The extra knowledge given in the second part is: *malicious apps might understand your position even if you have explicitly said that you do not want to be geolocated and turned GPS off.*

On average, the "high" option moved 30% to 77% ($p < 0.0001$). In details, male users (+37%, $p < 0.0001$), female users (+55%, $p < 0.0001$), Android (+42%, $p < 0.0001$), iOS (+61%, $p < 0.0001$), young adults (+50%, $p < 0.0001$) and adults (+39%, $p < 0.0001$). It is to highlight that the percentage of female participants who answered "no idea" passed from 29% to 0%, a clear indication that people ignored what can be done with the data. Similarly, iOS users moved from 30% to 91%.

Vibration. *"Rate the importance you give to the vibration feature when using a smartphone"*. The extra knowledge given in the second part is: *malicious apps might silence the vibration to delay your reading of possible warning messages such as bank account accesses.* On average, the "high" option moved from 8% to 61% ($p < 0.0001$). In details, male users (from 5% to 48%, $p < 0.0001$), female users (from 11% to 71%, $p < 0.001$), Android users (from 9% to 55%, $p < 0.0001$), iOS users (from 7% to 74%, $p < 0.001$), young adults (from 7% to 53%, $p < 0.0003$), adults (from 12% to 78%, $p < 0.0001$).

Running Apps. *"Rate the importance you give to the list of running apps when using a smartphone"*. The extra knowledge given in the second part is: *malicious apps might close security or antivirus apps in order to take control of your smartphone.* On average, the "high" percentage moved from 12% to 73% ($p < 0.0001$). In details, male uses (from 12% to 62%, $p < 0.0008$), female users (from 13% to 82%, $p < 0.0001$), Android users (from 12% to 71%, $p < 0.0001$), iOS users (from 15% to 81%, $p < 0.004$), young adults (from 13% to 66%, $p < 0.0001$), adults (from 12% to 90%, $p < 0.0005$).

Multimedia Storage. *"Rate the importance you give to the multimedia storage when using a smartphone"*. The extra knowledge given in the second part is: *malicious apps might access and download your personal pictures and videos.* On average, the "high" option moved from 57% to 79% ($p < 0.0003$). in details, male users (from 55% to 71%, $p < 0.03$), female users (from 59% to 85%, $p < 0.006$), Android users (from 53% to 74%, $p < 0.001$), iOS users (from 67% to 93%, $p = 0.1$ not significant), young adults (from 53% to 75%, $p < 0.005$), adults (from 67% to 86%, $p < 0.008$).

Camera. *"Rate the importance you give to the camera device when using a smartphone"*. The extra knowledge given in the second part is: *malicious apps might turn your camera on and record everything.* On average, the "high" option moved from 53% to 84% ($p < 0.0001$). In details, male users (from 60% to 77%, $p < 0.01$), female users (from 48% to 90%, $p < 0.0001$), Android users

(from 53% to 81%, $p < 0.001$), iOS users (from 56% to 91%, $p < 0.001$), young adults (from 48% to 83%, $p < 0.0001$), adults (from 65% to 84%, $p < 0.006$).

Location. *"Rate the importance you give to your location when using a smartphone"*. The extra knowledge given in the second part is: *malicious apps might know where you are and sell this info to third parties.* On average, the "high" option moved from 48% to 71% ($p < 0.001$). In details, male users (from 51% to 65%, $p < 0.02$), female users (from 46% to 76%, $p < 0.001$), Android users (from 48% to 64%, $p < 0.01$), iOS users (from 50% to 85%, $p < 0.01$), young adults (from 49% to 72%, $p < 0.001$), adults (from 45% to 67%, $p < 0.01$).

ID Smartphone. *"Rate the importance you give to the ID of your phone when using a smartphone"*. The extra knowledge given in the second part is: *malicious apps might know your telephone number and IMEI and might sell this info to third parties.* On average, the "high" option moved from 28% to 73% ($p < 0.01$). In details, male users (from 23% to 65%, $p < 0.001$), female users (from 32% to 79%, $p < 0.002$), Android users (from 26% to 68%, $p < 0.02$), iOS users (from 35% to 85%, $p < 0.01$), young adults (from 29% to 68%, $p < 0.003$), adults (from 25% to 80%, $p < 0.001$).

Network. *"Rate the importance you give to the Network information when using a smartphone"*. The extra knowledge given in the second part is: *malicious apps might download and install software without your permission.* On average, the "high" option moved from 12% to 74% ($p < 0.001$). In details, male users (from 8% to 68%, $p < 0.001$), female users (from 15% to 79%, $p < 0.001$), Android users (from 12% to 73%, $p < 0.04$), iOS users (from 13% to 80%, $p < 0.001$), young adults (from 10% to 68%, $p < 0.001$), adults (from 16% to 88%, $p < 0.002$).

SMS. *"Rate the importance you give to SMS when using a smartphone"*. The extra knowledge given in the second part is: *malicious apps might send/delete SMS without your permission.* On average, the "high" option moved from 63% to 78% ($p < 0.002$). In details, male users (from 52% to 73%, $p < 0.002$), female users (from 71% to 83%, $p < 0.01$), Android users (from 55% to 73%, $p < 0.001$), iOS users (from 78% to 89%, $p < 0.0001$), young adults (from 58% to 74%, $p < 0.002$), adults (from 75% to 88%, $p < 0.004$).

We conclude by observing that knowledge also affected volunteers initial perception. Indeed, some issues related to privacy have been discussed by media and educational institutions, and people are starting to understand possible misuse of some type of personal data: people is nowadays more aware than yesterday that they should be careful when spreading their contents (and the "high" option initially is at 57% for multimedia storage, and at 63% for SMS), people heard the "story" of how one can be spied through device cameras or microphones (and the "high" option is initially at 53% for camera, and at 46% for microphone), and people have been alerted of the dangers of being geolocated (and the "high" option is at 48% for location). On the contrary, no great debate addressed possible misuses of smartphone vibrations ("high" option initially at 8%), or network information ("high" option initially at 12%).

4 Analysis of Users' Behavior

4.1 Methodology

To evaluate H2, we asked for volunteers willing to share with us the list of the apps installed on their smartphones. Volunteers were recruited through friends, acquaintances, and family referrals using the snowball strategy. We have been contacted by 30 people: 60% male and 40% female, 71% young (below 30 year-old) and 29% adult (above 30 year-old), 86% with Android and 14% with iOS. The total number of installed apps amounts to 843, excluding those that usually might access to every single data on a smartphone such as the manufacture ones, network providers and OS developers apps.

We manually analyzed the authorizations requested by the 843 apps focusing on the same features of the previous section (contacts, microphone, Wi-Fi connections, vibration, running apps, multimedia storage and camera) in order to check if the apps requests go beyond their needs. When this happens, we might be facing data abuse.

4.2 Data and Results

Participants have few common applications: Whatsapp (87% of the participants has it on their smartphone), Telegram (68%), Facebook (60%), Spotify (60%), Instagram (60%), Dropbox (41%) and Skype (36%). In general, only 16% of the analyzed apps are installed on more than one smartphone, whereas 84% of the apps are used by a single volunteer. In details, the analysis of authorization requests by the 843 apps reveal an alarming scenario:

- **Contacts**. 24% of the installed apps access to this data and 39% of them violate the user's privacy;
- **Location**: 36% of the installed apps access to this data and 28% of them violate the user's privacy;
- **ID Telephone**: 8% of the installed apps access to this data and 68% of them violate the user's privacy;
- **SMS**: 7% of the installed apps access to this data and 37% of them violate the user's privacy;
- **Multimedia storage**: 56% of the installed apps access to this data and 29% of them violate the user's privacy;
- **Microphone**: 12% of the installed apps access to this data and 38% of them violate the user's privacy;
- **Wi-Fi connections list**: 33% of the installed apps access to this data and 52% of them violate the user's privacy;
- **Vibration**: 37% of the installed apps access to this data and 22% of them violate the user's privacy;
- **Running apps list**: 7% of the installed apps access to this data and 58% of them violate the user's privacy;

Table 2: Percentage of installed apps that might violate users' privacy.

	Male	Female	Android	iOS	Young adults	Adults
Contacts	13%	15%	15%	15%	13%	16%
Microphone	4%	14%	9%	12%	10%	11%
Wi-Fi Connection list	39%	33%	36%	35%	34%	38%
Vibration	3%	9%	6%	8%	8%	5%
Running Apps	11%	13%	10%	15%	12%	12%
MM Storage	17%	18%	20%	16%	16%	21%
Camera	17 %	25%	23%	20%	19%	26%

- **Photo camera**: 26% of the installed apps access to this data and 46% of them violate the user's privacy;
- **Video camera**: 14% of the installed apps access to this data and 64% of them violate the user's privacy;

With respect to the users' behavior, Table 2 shows an in-depth analysis related to different groups of people (i.e., male, female, android users, iOS users, young adults and adults). It can be noted that, among the possible abuses, there is clearly an unmotivated access to the list of wifi networks (probably due to the need to locate the user), but there are no groups that are more exposed than others to possible abuses. The most noticeable difference concerns the microphone where 4% of the male users are exposed to privacy violation, whereas 14% of female users are exposed to privacy violation.

5 Conclusions

In this paper, we investigated privacy perception and users' behavior in the mobile ecosystem. Our hypotheses: users ignore the relationship between authorization requests and privacy and this lack of knowledge affects their perception towards privacy (**H1**); users install applications that access sensitive data that are not necessary for their correct functioning (**H2**). To assess H1, we asked 200 volunteers to participate to three-phases experiment: 1) fill a questionnaire related to privacy perception and behavior; 2) listen to what applications might do with personal data; 3) answer to the same questions of phase 1. By comparing the overall perception before and after the introduction of extra knowledge, the obtained results statically confirmed H1 ($p < 0.0001$). Indeed, the majority of users changed their perception, showing that the lack of knowledge affects privacy perception. For instance, participants have little information about the Wi-Fi networks list, iOS users are surprised about a possible misuse of the vibration sensor, adults are concerned about the use of the running apps list, women have increased their concern about possible microphone and camera abuse. To assess H2, we asked 30 volunteers to share with us the list of installed apps and then we analyzed the permissions requested by these apps. By analyzing the 843 apps, we observed that users are subject to privacy abuses as installed apps access more sensitive data than necessary, confirming our hypothesis H2.

This study is the first step towards a safer mobile ecosystem as it identifies features relevant to specific types of users. By combining features and types of users, authorization requests can be more understandable and effective. For example, since adults are concerned about phonebook contacts and about the list of Wi-Fi connections, when an application requires access to this data, the authorization message should warn users about privacy risks.

References

1. Louis Brandeis and Samuel Warren. The right to privacy. *Harvard law review*, 4(5):193–220, 1890.
2. H Jeff Smith, Sandra J Milberg, and Sandra J Burke. Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, pages 167–196, 1996.
3. Shirin Elahi. Privacy and consent in the digital era. *Information security technical report*, 14(3):113–118, 2009.
4. J. Isaak and M. J. Hanna. User data privacy: Facebook, cambridge analytica, and privacy protection. *Computer*, 51(8):56–59, August 2018.
5. A. Bujari, M. Furini, and N. Laina. On using cashtags to predict companies stock trends. In *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 25–28, Jan 2017.
6. Marco Furini and Manuela Montangero. Sentiment analysis and twitter: a game proposal. *Personal and Ubiquitous Computing*, 22(4):771–785, Aug 2018.
7. Nicola Dusi, Ilaria Ferretti, and Marco Furini. A transmedia storytelling system to transform recorded film memories into visual history. *Entertainment Computing*, 21:65 – 75, 2017.
8. Lavinia Egidi and Marco Furini. Bringing multimedia contents into MP3 files. *IEEE Communications Magazine*, 43(5):90–97, May 2005.
9. Marco Furini, Giovanna Galli, and Maria Cristiana Martini. An online education system to produce and distribute video lectures. *Mobile Networks and Applications*, Mar 2019.
10. Maria Federico and Marco Furini. An automatic caption alignment mechanism for off-the-shelf speech recognition technologies. *Multimedia Tools and Applications*, 72(1):21–40, 2014.
11. Marco Furini and Roberta De Michele. On improving the engagement between viewers and tv commercials through gamification. *Multimedia Systems*, Jun 2019.
12. Roberta De Michele, Stefano Ferretti, and Marco Furini. On helping broadcasters to promote tv-shows through hashtags. *Multimedia Tools and Applications*, 78(3):3279–3296, Feb 2019.
13. Matthew Hettrich. Data privacy regulation in the age of smartphones. *TOuRO L. REv.*, 31:981, 2014.
14. I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proc. ACM Conf. on Human Factors in Computing Systems*, pages 2347–2356, 2014.
15. Armir Bujari, Marco Furini, Federica Mandreoli, Riccardo Martoglia, Manuela Montangero, and Daniele Ronzani. Standards, security and business models: Key challenges for the iot scenario. *Mobile Networks and Applications*, 23(1):147–154, Feb 2018.
16. Kathy Wain Yee Au, Yi Fan Zhou, Zhen Huang, and David Lie. Pscout: analyzing the android permission specification. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 217–228. ACM, 2012.
17. Marco Furini, Federica Mandreoli, Riccardo Martoglia, and Manuela Montangero. *IoT: Science Fiction or Real Revolution?*, pages 96–105. Springer International Publishing, Cham, 2017.
18. Roberta De Michele and Marco Furini. Iot healthcare: Benefits, issues and challenges. In *Proceedings of the International Conference on Smart Objects and Technologies for Social Good (GoodTechs 2019)*. ACM, 2019.

19. W. Meng, F. Fei, W. Li, and Man Ho Au. Harvesting smartphone privacy through enhanced juice filming charging attacks. In Phong Q. Nguyen and Jianying Zhou, editors, *Information Security*, pages 291–308, Cham, 2017. Springer International Publishing.
20. Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. Little brothers watching you: Raising awareness of data leaks on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 12. ACM, 2013.
21. P. Aditya, B. Bhattacharjee, P. Druschel, V. Erdelyi, and M. Lentz. Brave new world: Privacy risks for mobile users. In *Proc. ACM MobiCom Workshop on Security and Privacy in Mobile Environments*, pages 7–12, 2014.
22. M. Furini and V. Tamanini. Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions. *Multimedia Tools and Applications*, 74(21):9795–9825, 2015.
23. J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang. Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proc. ACM Conf. on Ubiquitous Computing*, pages 501–510, 2012.
24. Nurul Momen and Marta Piekarska. Towards improving privacy awareness regarding apps' permissions. In *11th International Conference on Digital Society (ICDS, Nice, France, March 19-23, 2017*, pages 18–23. International Academy, Research and Industry Association (IARIA), 2017.
25. Marco Furini. Users behavior in location-aware services: Digital natives vs digital immigrants. *Advances in Human-Computer Interaction*, 2014, 2014.
26. Susanne Barth and Menno DT De Jong. The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review. *Telematics and Informatics*, 34(7):1038–1058, 2017.
27. Marco Furini, Silvia Mirri, Manuela Montangero, and Catia Prandi. Privacy perception and user behavior in the mobile ecosystem. In *Proceedings of the 5th EAI International Conference on Smart Objects and Technologies for Social Good*, pages 177–182. ACM, 2019.
28. Alastair R Beresford, Andrew Rice, Nicholas Skehin, and Ripduman Sohan. Mockdroid: trading privacy for application functionality on smartphones. In *Proceedings of the 12th workshop on mobile computing systems and applications*, pages 49–54. ACM, 2011.
29. William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N Sheth. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)*, 32(2):5, 2014.
30. Wenyun Dai, Meikang Qiu, Longfei Qiu, Longbin Chen, and Ana Wu. Who moved my data? privacy protection in smartphones. *IEEE Communications Magazine*, 55(1):20–25, 2017.
31. H. Khalid, E. Shihab, M. Nagappan, and A. E. Hassan. What do mobile app users complain about? *IEEE Software*, 32(3):70–77, May 2015.
32. M. M. Baig, H. GholamHosseini, and M. J. Connolly. Mobile healthcare applications: system design review, critical issues and challenges. *Australasian Physical & Engineering Sciences in Medicine*, 38(1):23–38, Mar 2015.
33. M. Alenezi and I. Almomani. Abusing android permissions: A security perspective. In *IEEE Jordan Conf. on Applied Electrical Engineering and Computing Technologies (AEECT)*, pages 1–6, Oct 2017.
34. H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proc. ACM Conference on Human Factors in Computing Systems*, pages 787–796, 2015.
35. B. Liu, M. S. Andersen, F. Schaub, H. Almuhimedi, S. (A.) Zhang, N. Sadeh, Y. Agarwal, and A. Acquisti. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In 12^{th} *Symp. on Usable Privacy and Security (SOUPS 2016)*, pages 27–41. USENIX Association, 2016.