Politecnico di Milano

School of Industrial and Information Engineering

Master of Science in Management Engineering

POLITECNICO
MILANO 1863

Privacy and Data: How are mobile apps addressing Users' Privacy Concerns?

Supervisor

Prof. Daniel Trabucchi

Candidate

Paolo Borzone

919751

Academic Year 2019/2020

Questa tesi è dedicata a chiunque creda che il suo operato dia anche solo un piccolo contributo al mondo in cui viviamo. Sono sempre stato affascinato da cosa ci possono dire i dati e dal valore che possono celare, ma la storia di Cambridge Analytica mi ha portato a riflettere sulle conseguenze del loro uso improprio e sui pericoli e sulle sfide che il progresso ci sta ponendo davanti.

Ringrazio il mio supervisore Daniel Trabucchi per avermi dato l'opportunità di approfondire l'argomento e presentarlo come conclusione del mio percorso di studi al Politecnico di Milano, e per tutti i consigli e le idee che mi ha suggerito nel corso dell'ultimo anno.

Ringrazio mia mamma, mio fratello e Giulia per il continuo aiuto durante la mia esperienza universitaria, e Carlo, Mattia, Giovanni, Marco e tutti coloro che hanno vissuto con me questi anni indimenticabili in cui non si ho mai smesso di imparare e di divertirmi.

Table of contents

List of tables

List of figures

Abstract

Data are changing the world we live in, but the right to privacy of those generating them is often ignored for the sake of economic value. This research analyses if and how digital firms are shaping their value proposition in order to address their customers' need for privacy while offering services that are based on personal information.

The meaning of privacy and how it affects consumers' behaviour have been studied in order to design a theoretical model meant to assess how digital firms are implementing Information Transparency and Data Perceived Control in their offer to address Users' Privacy Concerns. The model has been applied to 71 of the 100 most downloaded Android applications and provided both quantitative and qualitative results.

On the one hand, it appears that firms are actually providing Transparency and Control in some ways to their users, mainly about which types of data are collected and how they are collected; app of the "Social" and "Communication" category are apparently leading the market in terms of Transparency and Control levels. Also, being transparent about data practices is generally preferred to allowing control over them.

On the other hand, some recurring strategies involving a proactive approach to the addressment of privacy concerns have emerged: almost half of the sample offers a certain degree of Transparency and Control before the users is allowed to start using the app. This approach is pursued with two possible channels, the Play Store page or the app initialization, and three non-exclusive strategies, depending on what is provided: information about data practices ("Information Only" strategy), warnings and explanations of what sensors and data of the device need to be accessed ("Authorization Heads-up" strategy) or some controls over data practices ("Early Control" strategy).

Abstract (Italian)

I dati e il loro utilizzo stanno cambiando il mondo in cui viviamo, ma spesso il diritto alla privacy di coloro che li generano, gli utenti, viene sacrificato in nome del profitto. Questa ricerca studia se e come le aziende digitali stanno cambiando la loro offerta di business per soddisfare il bisogno di privacy dei loro utenti, mentre continuano a offrire loro servizi personalizzati basati sull'analisi dei loro dati.

Il significato della privacy e il suo effetto sul comportamento dei consumatori sono stati studiati per progettare un modello in grado di valutare come le aziende stiano offrendo Trasparenza e Controllo ai loro utenti per affrontare le preoccupazioni generate dal bisogno di privacy. Il modello è stato quindi usato per analizzare 71 delle 100 app più scaricate del Play Store Android e per generare risultati sia quantitativi che qualitativi.

Nel primo caso, sembra che le app stiano effettivamente offrendo un certo livello di Trasparenza e Controllo (la prima in maggior misura) ai loro utenti, principalmente riguardante quali dati vengono raccolti e come. Tra le categorie più presenti nel campione, i Social e le app di messaggistica sono quelle che stanno seguendo questa strategia più insistentemente.

Nel secondo caso, sono state identificate alcune strategie di app che offrono Trasparenza e Controllo proattivamente, ossia prima che l'utente inizi effettivamente ad utilizzare l'app. Questo approccio viene seguito con due canali di comunicazione, la pagina di presentazione del Play Store o l'app stessa al primo utilizzo, e tre strategie dipendenti da cosa viene offerto, che può essere: semplici informazioni riguardo l'utilizzo dei dati (strategia "Information Only"), alcuni avvisi e spiegazioni riguardo a quali sensori e aree dello smartphone l'app deve accedere (strategia "Authorization Heads-up"), o alcuni controlli per decidere quali attività di raccolta, analisi e condivisione dati permettere (strategia "Early Control").

Executive Summary

Progress is constantly changing the world we live in: scientific and managerial innovation combine together to advance how today's economy regulates exchanges in the society, and the latest decade has seen new digital business models disrupting traditional value chains. Technological progress enabled the possibility to collect, read and analyse large amounts of information and gave birth to the Big Data paradigm: "Big Data" are data that are large in volume, heterogeneous, veracious, generated at high and variable velocity, and their analysis can generate relevant business value (Gandomi, et al., 2015; McAfee, et al., 2012).

In a world where everyone is connected thanks to the increasing diffusion of smart devices, every individual is a source of Big Data, and firms are easily capturing them to foster inbound and outbound innovation to unlock new sources of value creation (Trabucchi, et al., 2017b). User Generated Big Data (UGBD) outperform traditional techniques of user research, as they allow to collect information about consumers behaviour with low target's awareness and high contextuality (Trabucchi, et al., 2017b), resulting in an increasing integration of digital services providers in consumers life.

Big Data enabled the raise of new digital business models: two-sided platforms, which base their value proposition on the intermediation between two groups of customers and fuel it by processing information and internalizing externalities to let these two sides find each other in the market (Evans, 2003). Among them, non-transactional platforms are models that allow for an interaction between the two sides that does not present transactions. Instead, they generally charge the side that wants to communicate with the other (a typical example is the advertising business model) (Filistrucchi, et al., 2014).

The possibility to extract value from UGBD has enriched the possible revenue streams of non-transactional platforms: following a "Client as a Source" strategy, these platforms are using the data generated by one side of the two-sided market to (1) increase the effectiveness of advertisers targeting, (2) allow for innovative ways to collect insights about users' behaviour to support user research and (3) create a new revenue streams by selling data to third parties that can be interested in combining them with other information to generate additional value (Trabucchi, et al., 2017a).

All of these new strategies and the value they unlock are based on UGBD, but their exchange between the source (the user) and the utilizer (the firm) is poorly regulated by market mechanisms and laws. Recent scandals involving digital platforms, such as the story of how

data has been used to influence the American and British elections in 2016 by Cambridge Analytica (Kaiser, 2019; Wylie, 2019), raised the attention of public opinion and regulators on how these novel business models are using personal data to profit, and privacy is now a topic that cannot be ignored by firms basing their value proposition on UGBD.

Privacy is "the claim of an individual to determine what information about himself or herself should be known to others" (Westin, 1967), hence granting such claim means that innovative two-sided platforms cannot freely collect and use information generated by their users. The effect that the violation of privacy exerts on people are reflected on privacy concerns, which are the individuals' anxieties and beliefs associated with the information practices of the organizations (Smith, et al., 1996). Privacy concerns can be caused by the worries about whether and how data are collected, used, shared, can be corrected and are safely stored (Smith, et al., 1996).

Privacy concerns should be taken into account during the design of a value proposition based on UGBD, because they affect users' behavioural intention regarding the usage of digital services. In particular, privacy concerns are negatively associated with the willingness to disclose personal information (Sheehan, et al., 1999; Min, et al., 2015; Dinev, et al., 2006; Baruh, et al., 2017), to use digital services (Martin, et al., 2016; Bandyopadhyay, 2009; Bélanger, et al., 2011; Li, et al., 2012), and to purchase goods on digital markets (Smith, et al., 2011; Bandyopadhyay, 2009).

According to literature, firms can embed two levers in their offer to mitigate the effects of privacy concerns over behavioural intention: Information Transparency and Data Perceived Control. Information Transparency is "the degree to which an individual can access the information that a firm has collected about him or her and understand how that information is going to be used" (Awad, et al., 2006), while Perceived Data Control (PDC) is the consumers' perception of their ability to manage the collection and use of their personal information (Libaque-Sáenz, et al., 2020; Xu, et al., 2011). At least in Europe, both levers must be implemented in some way to comply with the latest law regarding data practices, the General Data Protection Regulation (European Union, 2016). Also, their adoption was already advocated by the Fair Information Practices, in the form of the Notice, Access and Choice principles (Organization for Economic Cooperation and Development, 1980; Federal Trade Commission, 2020). However, there are not rigid guidelines regarding the depth with which transparency and control must be integrated in digital services, resulting in variable levels of transparency and control in the market (Bornschein, et al., 2020; Schwaig, et al., 2006).

Including transparency in the business model positively affects the willingness to use a service for individuals with high privacy concerns. Additionally, its effect on the willingness to use the service is extendable to all users in case they are aware of the existence of a transparent business model as an alternative to the classic opaque ones (Trabucchi, et al., 2019).

On the other hand, Perceived Data Control has been proven to be a successful lever to reduce privacy concerns, mitigate the effects they have on behavioural intention, or to directly increase such intention (Chang, et al., 2018; Dinev, et al., 2013; Dinev, et al., 2006; Libaque-Sáenz, et al., 2020; Bornschein, et al., 2020; Tucker, 2014).

Transparency and Control hav been often addressed together by both researchers (Sheehan, et al., 2000; Foxman, et al., 1993; Martin, et al., 2017) and regulators (European Union, 2016; Federal Trade Commission, 2020), and firms should follow their example, because knowledge has been shown to be a determinant of perceived control (Armitage, et al., 1999; Ajzen, et al., 1991; Wortman, 1975), and few results show that transparency without control may be detrimental to behavioural intention (Bornschein, et al., 2020; Martin, et al., 2017).

The following research has been designed to evaluate if and how firms that collect and leverage UGBD are addressing the rising privacy concerns of citizens by implementing Transparency and Control in their value propositions. In particular, it will answer the following research questions:

RQ1: Are firms leveraging data driven business models implementing Transparency and Control in their value proposition to address rising privacy concerns?

RQ2: What are the current levels of Transparency and Control offered by the most relevant players in the market?

RQ3: What dimensions of Privacy Concerns are addressed the most through Transparency and Control?

RQ4: Are there any industry-related trends regarding Transparency, Control, and how they are used to address Privacy Concerns?

RQ5: Are there any recurring strategies regarding the addressment of Privacy Concerns among firms leveraging data driven business models?

In order to answer such questions, a framework capable of assessing the addressment of privacy concerns trough Transparency and Control has been designed and applied to a representative sample of the subject of the research, which are firms pursuing a digital strategy based on data collection, sharing and analysis. The sample has been extracted from the 100 most installed ever android applications: applications available for download and offering a UI to let the user interact and take advantage of their features (71 of the original sample) have been downloaded and thoroughly tested looking for informative messages explaining data practices and options to control such practices.

The assessment model has been designed to measure the level of transparency as the number of informative messages regarding distinct data practices involving distinct types of data and the level of control as the number of options allowing the user to control distinct data practices over distinct types of data.

In order to assess how the two levers are used to address different privacy concerns, four area of measurement based on literature on privacy concerns have been defined: (1) Collection, for information and options regarding the gathering of data and their type; (2) Usage, for information and options about why data are collected and how they are used by the collector; (3) Sharing, for information and options regarding which data are shared, why and with whom; (4) Access, for visibility and possibility to modify or eliminate specific information that have been collected.

Findings are summarized as a series of 8 indicators (2 levers for 4 areas of measurement) for each unit. Then, the overall levels of transparency and control have been computed by summing the 4 indicators associated to the same lever. Additionally, if both metrics were not null, the ratio between the transparency and the control has been computed.

The discussion is divided in two parts: the first one applies a quantitative approach to the evidence gathered to answer RQ1, RQ2, RQ3 and RQ4, while the second one presents a qualitative analysis of recurring strategies that the data collection process allowed to spot.

The quantitative analysis is based on descriptive metrics regarding the indicators that have just been described. Apparently, most of the market is actually offering transparency and control in the value proposition in order to mitigate privacy concerns. The large majority of the sample addresses privacy concerns with some information regarding how the data are treated (87%) and some options that give the users power over these activities (81%). Still, the majority of the sample present a level of transparency and control lower than the average, meaning that the

market is populated with many players offering low transparency and control together with few providers implementing strongly the two mediators in their offer.

Transparency has a predominant role over control, consistently with literature, and the two levers present a certain degree of correlation, even if some players clearly preferring one mediator to the other have been spotted. Among privacy concerns, Collection is the most addressed one; Usage present a higher dominance of transparency over control, while both Sharing and Access present a Transparency/Control ratio close to 1.

Finally, the app belonging to the "Social" and "Communication" are the ones with the highest levels of transparency and control, consistently with the high interest these business model have on behavioural intention and the high concern they are currently associated to for public opinion.

The second part of the discussion presents proactivity strategies to Transparency and Control. A pattern of apps providing information and options before the user actually starts to use the service has emerged during the data gathering process. Apparently, almost half of the sample uses either their Play Store page or the app first opening to inform the users about data practices adopted or offering some ways to control them. Three possible and not exclusive strategies have been identified and are reported: players are applying a proactive approach to Transparency and Control by offering (1) simple notification about how data will be treated, without any control about it; (2) some insights and customized controls about which sensors and information of the device the app needs to access; (3) some options to customize how data will be treated already available in the service initialization.

In conclusion, firms leveraging data driven business models are currently including transparency and control in their value proposition, as two levers to mitigate the effects of privacy concerns on behavioural intention. The new regulatory frameworks and the raising interest of public opinion on data is influencing the market of digital services, and new practices addressing privacy are emerging. Giving users knowledge and power over their data is already being used as an attribute to differentiate from the market, in addition to complying with law.

1. Introduction

In 1890, Warren and Brande highlighted how "recent inventions and business methods call attention to the next step which must be taken for the protection of the person". They argued for the need to recognize privacy as "the right to be let alone" (Cooley, 1880) as an answer to an evolving environment in which "instantaneous photographs and news-paper enterprise have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops".

Their words fit very well with today's world, where information is being collected and processed in vast amount. Technological progress unlocked the possibility to collect and analyse vast amounts of information, the so called "Big Data", and that is profoundly changing the society we live in. In the last decade, Big Data fostered the innovation of digital services and disrupted many industries, empowering a new class of firms, the Big Bang Disruptors (Downes, et al., 2014) and innovative business models based on platforms (Parker, et al., 2017). Thanks to the value embedded in data and the possibility to extract it, firms are now capable of offering high quality and personalized services at a minimal (often null) price.

Because of the novelty of such practices, firms have pursued them unrestrained, collecting, sharing and processing data without worrying about the privacy rights of those who generate such data, the users. Eventually, the attention of public opinion and regulators rose up when the exploitation of Big Data had already resulted in drastic effects on society. On 17 March 2018, both the New York Times and The Guardian exposed how a company called Cambridge Analytica harvested personal data of more than a 50 million American users to influence the 2016 elections (Rosenberg, et al., 2018; Cadwalladr, et al., 2018). The scandal spiced up the debate about how firms are allowed to treat data and called for the need of regulatory systems capable of protecting the internet users' rights.

This research has been designed to evaluate if and how digital providers leveraging Big Data are addressing the users' right to privacy. Existing literature on privacy and how it affects consumers' behaviour has been reviewed and resulted in a theoretical model designed to assess how firms are addressing privacy concerns by implementing in their value propositions two major mediators of privacy concerns: Information Transparency and Data Perceived Control.

2. Literature Review

2.1 Data

Big Data

The term Big Data generally refers to a technological paradigm that emerged back in the 90s as a consequence of the increasing availability of data on a large scale (Diebold, 2012). The trend's relevance went on rising in the past decade and several definitions emerged causing a misalignment on the meaning of the term (Gandomi, et al., 2015): for example, Big Data have been identified as "the increase in volume and the difficulty to handle information" (Hashem, et al., 2015), "data that are too large in volume to be processed" (Manyika, et al., 2011) or "the new generation of technologies and architectures, designed to economically extract value from very large volumes of a wide variety of data, by enabling the high velocity capture, discovery, and/or analysis" (Gartner).

However, these definitions and many more converge around of a series of "V" properties that aggregations of Data need to satisfy in order to be considered "Big Data" (Gandomi, et al., 2015; Hashem, et al., 2015; Buganza, et al., 2019): the first set of properties belongs **the 3Vs model** (McAfee, et al., 2012) and are: Volume, which refers to dimensions of the data considered (measured in bytes), Velocity, which is the high rate at which data are generated and analysed and Variety, because Big Data are typically heterogenous and non-structured.

More recently, additional properties have been added to this classification (Gandomi, et al., 2015; Fan, et al., 2013; Kaisler et al., 2013; Wamba-Fosso, et al., 2015; Del Vecchio, et al., 2018): Value, that is the business value that the analysis of large quantities of data can generate, Veracity, that refers to the variable reliability of data, calling for ad hoc techniques and large datasets to extract reliable information, and Variability, which is not referred to the content (as Variety does), but to the variable Velocity trough which data are generated.

In the past years, numerous technological trends contributed to the increase of Big Data relevance: the diffusion of devices capable of generating and sharing large amount of information (Lohr, 2012), which has been furtherly boosted by the Internet of Things (Atzori, et al., 2010) and the continuous adoption and performances improvement of the cloud computing paradigm (Marston, et al., 2011), together with the decreasing costs of computational power (Vajjhala, et al., 2016).

Big Data are already affecting several managerial practices across different stages of the value chains of multiple industries (Trabucchi, et al., 2018), including the management of the

relationship between companies and their end users. This is possible because Big Data set the stage for the transformation of the firm-customer relationship, since end-users are today a relevant source of Big Data: they produce information as a by-product of their interaction with companies and this information are generally referred to as "User Generated Big Data" (UGBD) (Trabucchi, et al., 2017b).

The consumption of a service or a product nowadays generates valuable information that firms can collect and process, and the source of them is generally unaware of the digital marks it is leaving behind. Most of the time, the generation of data is necessary to obtain the service, hence users typically give up their information carelessly in order to enjoy a service or a product (Trabucchi, et al., 2017b). For example, an Amazon user generates data about what they are interested in just by using the platform and looking for something to buy or making purchases. Then, the firm combines this information to make suggestions to customers or even to pre-ship the products to the nearest hub waiting for the order to be placed (anticipatory shipping) (Erevelles, et al., 2016). An additional factor that is contributing to the easiness to collect UGBD is the diffusion of smartphones, which enable firms to gather large and heterogenous amounts of data with high speed and low user awareness (Buganza, et al., 2015).

UGBD can represent a valuable tool to power user-centred innovation, as they can outperform traditional techniques of user research in several ways. They are less expensive, highly replicable, generated by users themselves rather than reported by an intermediary and collectable with low user's awareness (thus reducing the possibility of biased results) in the real use contexts (thus increasing their meaningfulness) that can include also among-users' interactions (Trabucchi, et al., 2017b).

Firms are currently using UGBD to foster user centred innovation with two strategies (Trabucchi, et al., 2017b):

- "Using data" to improve the value proposition by both enlarging the bundle of activities offered in a service and moving to adjacent activity chains. For example, Deliveroo and Sportify use UGBD to offer customized services (restaurants suggestion or playlists) based on users' interaction with them.
- "Selling data" to external partners with different business models for which data generated in external industries (but relating to the same users) can unlock new revenue streams or enhance the value proposition. For example, Strava sells anonymized data

about the tracking habits of its users to municipalities that need to renew the city routes' structure.

The possibility to leverage UGBD to shape new value propositions has led the way to the rise of new business models grounded on Big Data, called "Data Driven Business Models" (Hartmann, et al., 2016). In particular, firms basing their business model on the two-sided market strategy have recently started to disrupt the digital market and consumers habits.

Two-sided platforms

Two-sided platforms are a data driven business model offering a double value proposition to two-sided markets: they generate value by enabling the interaction of two groups of customers and appropriately charging each side. In particular, a two-sided market presents (Evans, 2003):

1. Two or more distinct groups of clients;
2. Indirect network externalities associated with those groups;
3. An intermediary who can internalize the externalities.

Additionally, players of two-sided markets can be categorized as (Filistrucchi, et al., 2014):

- Transactional platform, if they allow an exchange between two actors and profit by asking a fee over the value of the transaction;
- Non-transactional platform, if the enabled interaction is a unilateral communication between one side and the other (e. g., audience and advertisers) and the platform profits by charging one side to communicate with the other.

Intermediation is not a new business model, but Big Data and the increasing easiness to collect and valorise UGBD is acting as propellent for firms leveraging a two-sided platform strategy. In particular, non-transactional platforms are unlocking new strategies based on the data generated by the accessed side. Not only these platforms are able to generate value by charging customers that need to access a particular segment ("Client as a target" strategy), but they are also generating value from the collection and analysis of the UGBD of the targets ("Client as a source" strategy) (Trabucchi, et al., 2017a; Trabucchi, et al., 2017b; Trabucchi, et al., 2019).

According to the latest research on Client as a Source models, these two-sided platforms can harvest value from UGBD in three ways (Trabucchi, et al., 2017a):

- Enhancing Client as a Target models by offering additional information on customer segments and enabling advertisers to target more effectively their customers (*Enhanced Advertising*);

- Providing insights into customer's behaviour that can support user research and foster innovation (*E-Etnography*);
- Selling these data to third parties that are able to exploit them to generate value, maybe by combining them with additional information they are gathering inside their process or elsewhere (*Data Trading*).

Big Data are rapidly changing how digital services create value and are allowing for an always more pervasive interaction with consumers. How their data are collected, analysed and used for profit is starting to be subject of debate, also because of recent scandals involving firms following two-sided market strategies and using UGBD to enrich their value proposition. Data privacy and how it is addressed is starting to affect consumers' behaviour, and its importance for players adopting Client as a Source strategy is likely going to increase in the next years (Trabucchi, et al., 2019).

2.2 Privacy constructs

Privacy

The oldest definition of privacy is "the right to be let alone", which has been firstly coined by Cooley (1880) and successively advocated by Warren and Brande (1890). The conceptualization of privacy as a right has been sustained also by the U.S. Supreme Court which described the "right to be let alone" as "the most comprehensive of rights, and the right most valued by civilized men" (U. S. Supreme Court, 1928) and used as the basic definition of privacy by different scholars (e.g., Hamid R. Nemati, 2009; Grzegorz Mazurek, 2019; Chang Liua, 2005). Nevertheless, the most adopted definition is the one provided by Westin: privacy is "the claim of an individual to determine what information about himself or herself should be known to others" (Westin, 1967). This definition refers specifically to the information belonging to an individual and the control he or she has over it (Fox, et al., 2018), therefore literature generally refers to this conceptualization of privacy as "informational privacy".

The difficulty in finding a univocal definition arises because "privacy is a plurality of different things and that the quest for a singular essence of privacy leads to a dead end" (Solove, 2008). Solove has investigated the multiple nature of privacy and listed six conceptualization of it: "(1) the right to be let alone; (2) limited access to the self, the ability to shield oneself from unwanted access by others; (3) secrecy, the concealment of certain matters from others; (4) control over personal information, the ability to exercise control over information about oneself; (5) personhood, the protection of one's personality, individuality, and dignity; and (6) intimacy, control over, or limited access to, one's intimate relationships or aspects of life". Basically, literature investigates privacy as a right in its fourth conceptualization, using the term "informational privacy" defined as "the ability (i.e., capacity) of the individual to control personally information about one's self" (Stone, et al., 1983; Clarke, 1999; Li, et al., 2012; Kokolakis, 2017; Hunter, et al., 2020).

Privacy Concerns

Most of the empirical privacy research has relied on privacy concern as a proxy for privacy because of the near impossibility to directly measure it (Smith, et al., 2011). Privacy concerns are individuals' anxieties and beliefs associated with the information practices of the organizations (Smith, et al., 1996) or, more specifically, their perceptions of what will happen to the information they provide to the organizations via internet (Malhotra, et al., 2004; Dinev, et al., 2006). In other words, privacy concerns are the manifestation of the people's need for the right to privacy to be granted.

In order to measure information privacy concerns. Smith and colleagues (1996) developed and tested the Concern for Information Privacy (CFIP) scale, which is composed of a 15 items list describing 4 dimensions of privacy concerns: Collection, Unauthorized secondary use (internal and external), Improper access and Errors. *Collection* is the "concern that extensive amounts of personally identifiable data are being collected and stored in databases", *Unauthorized secondary use* is the "concern that information is collected for one purpose but is used for an additional purpose inside (*internal*) or outside (*external*) the collecting organization". *Improper access* is the "concern that data about individuals are readily available to people not properly authorized to view or work on this data" and *Error* is the "concern that protections against deliberate and accidental errors in personal data are inadequate" (Smith, et al., 1996). The scale has then been tested by Stewart and Segars (2002), who have empirically confirmed its psychometric properties, and widely adopted by information privacy researchers (Malhotra et al. 2004; France Bélanger and Robert E. Crossler 2011; Xu et al. 2012).

Malhotra and colleagues (2004) developed the Internet User Information Privacy Concern (IUIPC), an adaptation of the CFIP scale to the internet domain. The new scale is based on Social Contract theory, whose application to information privacy suggests that "a firm's collection of personally identifiable data is perceived to be fair only when the consumer is granted control over the information and the consumer is informed about the firm's intended use of the information". The notion of IUIPC has been characterized in terms of three factors: *Collection, Control* and A*wareness*. Basically, IUIPC are conceptualized as "the degree to which an Internet user is concerned about online marketers' *collection* of personal information, the user's *control* over the collected information, and the user's *awareness* of how the collected information is used". Malhotra and colleagues used both IUIPC and CFIP scales to examine the relationship between privacy concerns and behavioural intentions and concluded that the first framework "includes and extends" the second, at least in the internet context. Nevertheless, "the majority of research related to privacy concerns still utilizes CFIP" (Bélanger, et al., 2011).

During the past years, privacy concerns have been investigated within a multitude of theories and framework aiming at describing the psychology of privacy. Researchers investigated what causes or mitigates privacy concerns, what are their effects and what mediates them (Smith, et al., 2011; Martin, et al., 2016; Li, 2012).

Behavioural intention

The effects of privacy concerns (privacy outcomes) are generally studied through the construct of behavioural intention, which is the person's volitional behaviour and can be used as a proxy for actual behaviour, according to the theory of reasoned action (Li, 2012; Ajzen, et al., 1975). In the privacy domain, behavioural intention has been referred to purchase intention (Smith, et al., 2011; Bandyopadhyay, 2009), willingness to disclose personal information (see next paragraph) and willingness to use a digital service (Martin, et al., 2016; Bandyopadhyay, 2009; Bélanger, et al., 2011; Li, et al., 2012).

Willingness to disclose

The relevance of the willingness to disclose personal information has increased, because of the raising relevance of customers' information in the most recent business models, and different scholars investigated whether an increase in privacy concerns led to a decrease in willingness to disclose. As individuals' concern with privacy increased, the likelihood of registering for a website requesting personal information decreases (Sheehan, et al., 1999). The negative relationship between privacy concerns and willingness to disclose has been validated both in the social network context (Min, et al., 2015) and in internet transactions (Dinev, et al., 2006). Baruh and colleagues (2017) performed a meta-analysis using the correlation coefficient as the main outcome metric and a random-effects model with restricted maximum likelihood estimator. The research included 166 studies investigating privacy concerns between 1990 and 2016, and it confirmed the negative correlation between privacy concerns and intentions to share personal information (r=−0.17, 95% CI [−0.27, −0.07]).

The literature investigating privacy concerns and willingness to disclose typically does not take into account actual behaviour. Instead, researchers infer it from behavioural intention (e.g. Malhotra, et al., 2004) through references to the Theory of Reasoned Action (TRA). TRA suggests that a person's volitional behaviour is determined by the person's behavioural intention to perform that behaviour, and behavioural intention is in turn determined by the person's attitude toward the behaviour and subjective norm (Ajzen, et al., 1975; Li, 2012).

This gap caused the opening of a relevant stream of research in the information privacy literature investigating the discrepancy between behavioural intention to disclose information and actual behaviour. (Norberg, et al., 2007) coined the term "privacy paradox" to describe such phenomenon and demonstrated the existence of a mismatch between what the subjects of their experiments said regarding their intentions and how they behaved successively. One of the causes appears to be the different effect that perceived risk have on willingness to disclose

compared to actual behaviour: it reduces the first one but has no effect on the latter. Acquisti (2004) had already analysed the phenomenon and claimed that the reason behind its existence lies in *bounded rationality*: people do not behave rationally when it comes to personal privacy, as they suffer from the *immediate gratification bias.* According to his theory, future privacy risks are undervalued when compared to present benefits (e.g. a discount or a personalized service) and thus people's behaviour is not affected by privacy concerns as much as they state.

Many researches provided results supporting the *privacy paradox* theory, but there are also many studies challenging it, showing that privacy concerns actually affect people's behaviour. The possible reasons behind this misalignment lie in the interpretation of the results, the context in which subjects are studied, the type of personal information, the research methodology (survey or experiment) and finally the model structure (Kokolakis, 2017).

Transparency

Information transparency is "the degree to which an individual can access the information that a firm has collected about him or her and understand how that information is going to be used" (Awad, et al., 2006). In other worlds, data transparency can be described as the "customer knowledge of a firm's access to her or his data and understanding of how it is going to be used". According to Gossip theory, which describes how people respond to the unsanctioned collection, use, or disclosure of their personal information (Dunbar, 2004; Foster, 2004), transparency is one of the factors that suppresses negative effects of unsanctioned transmissions of information and is described as "the target's awareness of which information about him or her is being shared" (Martin, et al., 2017).

Trabucchi and colleagues (2019) included the transparency construct in business model research as the "clarity in openly declaring if and how a firm leverage user-generated data". They defined a business model as transparent "when the service provider clearly declares in the service presentation how the gathered data are going to be used".

Transparency has recently received a major endorsement by EU regulation. The General Data Protection Regulation (GDPR) (European Union, 2016), shifted the role of transparency from an emerging business practice to an actual law affecting all firms operating in the EU and all people living there. In fact, the explicit requirement of transparency is one of the major changes of the GDPR compared to its predecessor, the Data Protection Directive of 1995. It required personal information to be "processed fairly and lawfully" (art. 12), which is extended by the GDPR by adding the expression "and in a transparent manner" (art. 13) to it (Ataei, et al.,

2018a). The processing is fair and transparent if the data subject is given notice of the existence of the processing and its purposes. Ensuring fairness and transparency regarding the lawfulness of the processing is thus achieved by informing data subjects about their rights, the consequences of their decisions, and the activities of the controller (Ataei, et al., 2018a). Transparency does not encompass only what the citizen must be notified of, but also how: the principle of transparency requires that any information and communication relating to the processing of those personal data must be easily accessible and easy to understand, and that clear and plain language must be used (Raschke, et al., 2018).

Control

In the psychology literature, control is commonly treated as a perceptual construct because perceived control affects human behaviour much more than actual control (Skinner, 1996). Perceived control has been generally defined as an individual's beliefs about the presence of factors that may facilitate or hinder the outcomes of the behaviour (Ajzen, 2001).

The involvement of control in privacy research may appear straightforward: if transparency is the knowledge and the understanding of information practices, control involves the consumers in the decision process. Privacy is the right to determine what individual information is disclosed (Westin, 1967), so it requires the individual to have control over it. In fact, control is one of the dimensions about which internet user can be concerned about, when considering information practices (Malhotra, et al., 2004).

However, researchers in law and social science have noted that it is important to treat control and privacy as two separate and supporting concepts (Margulis 2003a; Margulis 2003b; Solove, 2002). According to Waldo and colleagues (2007, p.61) "control over information cannot be the exclusive defining characteristic of privacy" and privacy is more than control.

Because of the ambiguity of the relationship between the two concepts, multiple conceptualizations of control have been pursued in privacy research (Xu 2012; Margulis 2003b). According to Xu (2012), control has been defined as the choice to opt out of an information exchange (Milne, et al., 2000) or the ability to affect the dissemination and use of personal information (Phelps, et al., 2000). Generally, research converged towards the interpretation of control as the ability of consumers to voice or exit in order to influence changes in organizational privacy practices they find to be objectionable (Malhotra, et al., 2004). Privacy literature has operationalized control through Perceived Data Control, which is

defined as the consumers' perception of their ability to manage the collection and use of their personal information (Libaque-Sáenz, et al., 2020; Xu, et al., 2011).

The relationship between Transparency and Control

Transparency and Control have been often studied together, as they are two strongly intertwined mediators of privacy concerns who concur to the respect of the right to privacy. Privacy is the right for the individual to determine what information about themselves should be known to others, hence firms must offer to their customers the possibility to control what information is collected. However, that is properly possible only if users have knowledge about the nature of these practices, meaning that firms have to be transparent about them. Therefore, being transparent and offering control to their customers are two not optional practices for firms for the privacy right to be granted.

Knowledge has been shown to be a determinant of perceived control (Armitage, et al., 1999; Ajzen, et al., 1991; Wortman, 1975), and the conventional marketing approach suggests that awareness of information collection is one of the two expressions of control and is the predominant influence on the degree to which consumers experience privacy concern, together with information usage (Sheehan, et al., 2000). Control is also the second factor that, together with transparency, suppresses the negative effects of unsanctioned transmissions of information, according to Gossip theory (Martin, et al., 2017).

Foxman and Kilcoyne (Foxman, et al., 1993) used the two dimensions of knowledge and control to classify four consumer privacy states. Specifically, they distinguished the privacy states operationally accordingly to who controls consumer data and whether consumers are informed about data collection and privacy rights.

Social Contract theory indicates informed consent and right of exit and voice as two fundamental requirements for norm-generating microsocial contracts (Dunfee, et al., 1999). Its application to the information privacy domain suggests that a firm's collection of personally identifiable data is perceived to be fair only when it is transparent and offers control to the user. In fact, transparency and control directly address two of the three factors characterizing Internet User Information Privacy Concerns described by Malhotra and colleagues (2004) as *awareness* and *control*.

Regulatory frameworks

Transparency and control are combined not only in research, but also in institutional guidelines and laws promoted by authorities in defence of citizens privacy rights.

Back in 1980, the Organization for Economic Cooperation and Development ("OECD") introduced for the first time the Fair Information Practices ("FIPs"), a set of internationally recognized practices for addressing the privacy of information about individuals that were already advocating for transparency and control. FIPs are procedures that provide control over the disclosure and subsequent use of personal information and govern the interpersonal treatment that consumers receive (OECD, 1980). Currently, the most widely accepted U.S. definition, provided by the Federal Trade Commission (2000), of Fair Information Practices reflects a subset of the OECD Guidelines and is based on four elements:

- *Access*: Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review the information and to correct inaccuracies or to delete information;
- *Security*: Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers;
- *Choice*: Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities);
- *Notice*: Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g. directly or through non-obvious means such as cookies), how they use it, how they provide *Choice*, *Access*, and *Security* to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.

The comparison of FIPs with the definition of transparency and control highlights a clear overlay:

- *Transparency* incorporates the principle of *Notice* and part of the *Access* one (the possibility to view the collected information);
- *Control* includes both the principle of *Choice* and the possibility to review the collected information of the *Access* principle.

Over the years, the Fair Information Practices have been subjects of numerous privacy studies: they are principles that balance the legitimate need for business to collect and use personal

information with the privacy interests of consumers to be able to exercise control over the disclosure and subsequent use of their personal information (Culnan, et al., 2003).

The utilization of FIPs exerts an influence on consumers' privacy assessment in their intention to adopt mobile apps. Apparently, when consumers are aware that firms provide them with notice, choice, access and security their perceived data control increases, the perceived risks decrease and finally behavioural intention (in terms of willingness to use) rises (Libaque-Sáenz, et al., 2020). When fair procedures in the form of Fair Information Practices are observed, the negative effect of privacy concerns over willingness to be profiled for personalisation is suppressed. However, that does not have the same effect on previous past experiences. When fair information practices are observed, customers will be more willing to continue in a relationship with a firm, allowing the firm to benefit from the collection and use of data that results from the relationship (Culnan, et al., 1999).

The GDPR advanced and put into law what was already present in FIPs, as it enforces both the right to transparent treatment and control over personal data, by obliging data controllers to give users notice, consent and control about data processing (Ataei, et al., 2018a).

- Notice requires the communication of the data subjects of the existence of the processing and its purposes and other valuable information like the identity and the contact details of the controller, where the processing is based, the period for which the personal data will be stored, the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved;
- Consent is "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them" (GDPR, Article 4). The data subject shall have the right to withdraw his or her consent at any time (GDPR, Article 7) in a manner that is as easy as granting it;
- Control includes various rights that the consumer has on the data collected about them, such as the right to access, rectify and erase the data, the right to restriction, the right to data portability and the right to object.

Even if consent is here distinguished by control, the two constructs are clearly connected and the second typically encapsulates the first one in privacy literature. The need for consent to be informed: "the consent is informed if the data subject is aware at least of the identity of the

controller and the purposes of the processing for which the personal data are intended" (GDPR, 2016) is again a validation of the importance of transparency on control and privacy.

Operationalization

The definition of transparency and control is not univocal, but rather fragmented in multiple and overlaying constructs with recurring content. They have been advocated in regulatory frameworks, like GDPR and FIPs, under the concepts of Notice, Consent, Choice, Access and others, and their effects on behavioural intention have been studied in numerous privacy researches. The relationships of such construct is summarized below.

Right	Privacy		
Mediators	**Transparency**	**Control**	
FIPs	Notice	Access	Choice
GDPR	Notice	Consent	Control
IUIPC	Awareness	Control	

Table 1: Privacy constructs relationship

In order to obtain a clear definition of the two mediators, which are ultimately going to be the two unit of analysis of this research, the review of the operationalization of the two variables (and of the other constructs they include) is here reported.

Transparency generally refers to a communication between the firm and the consumer. Hence, researchers have operationalized its measurement with a list of information that are supposed to be included in the disclosure, combined with how this information are notified and in which context.

Awad and colleagues (2006) operationalized the "Importance of information transparency" as: (1) importance of whether a site is going to use the personal information they collect in a way that will identify the individual, (2) importance of know how long a company will retain information they collect from the individual, (3) importance of knowing what information a company keeps about the individual, (4) importance of why, for what purpose, the company is collecting personal information.

Trabucchi and colleagues (2019) defined a business model as transparent if the firm declares how it leverages the gathered data through a series of descriptive messages in the service presentation (the first opening of the application), in addition to having a GDPR-abiding

privacy policy. A similar approach had been followed by (Culnan, et al., 1999), who modelled a situation with a transparent website, by describing to respondents a service provider which, before letting the user subscribe, would fully inform him/her about the collection of his/her profile information and how it would be used.

When compared to information transparency, in the control research there is a higher convergence on the operationalization of perceived data control. The majority of surveys (e.g., Dinev, et al., 2013; Chang, et al., 2018; Xu, 2007; Xu, et al., 2011; Libaque-Sáenz, et al., 2016; Libaque-Sáenz, et al., 2020) measured PDC by asking the respondents whether they believed to have control over:

- Who can access their personal information;
- What type of personal information is collected by firms;
- How personal information is used by data collecting firms;
- What personal information is released by data collecting firms;
- The information collected by data collecting firms (i.e., they can modify it once it has been collected).

In the majority of studies, transparency and control have been evaluated through the concepts of Notice, Choice and Access principles of the FIPs: Bornschein and colleagues (2020) evaluated the degree of Transparency and Control offered in the cookie notices of 343 website among the 10’000 most visited ones by distinguishing different levels for:

- Notice: (1) absent, if no cookies notice were displayed on the website, (2) low visibility, if the notice was presented as a bar at the bottom of the screen, (3) high visibility, if the notice was a highly visible fly-in overlay;
- Choice: (1) information-only, if the cookie notice existed, but did not give any option, (2) universal consent, if there was the possibility to accept or decline data collection overall, (3) mixed consent, if it was possible to keep active only a subset of cookies, allowing the collection of only certain types of data.

Libaque-Sáenz and colleagues (2020) operationalized the implementation of the FIPs by explicitly telling the subjects that the app they were evaluating had a "Privacy Suite" that allowed them:

- For *Notice*, to revise the app's practices in the use of their personal information;
- For *Consent*, to give or withhold their consent to use specific personal data about them (e.g., name, occupation, gender, age, and e-mail) without affecting the use of the app;
- For *Access*, to correct information about their information collected by a third-party e-commerce operator.

Nemati and collegaues (2009), instead, analysed the privacy policy and checked whether the firm specified:

- For *Notice*, (1) what information is collected, (2) how information is collected, (3) how information is used. In particular, all the requirements had to be satisfied for the principle to be considered correctly adopted;
- For *Access*, how the user can review or change personal information;
- For *Choices*, whether the firm provides (1) opt-out option for internal use, (2) opt out-option for 3rd party use, (3) opt in for 3rd party use. In particular, if any of the three requirements was true the site satisfied the requirements for choice.

Both Wua (2012) and colleagues and Chang and colleagues (2018) (Wua, et al., 2012) and used the same criteria, but with different requirements. They checked in the privacy policy whether:

- For *Notice*: the firm (1) discloses what personal information is going to be collected, (2) explains why personal information is going to be collected, (3) explains how the collected personal information will be used;
- For *Access*: the firm allows the user to (1) review collected personal information, (2) correct inaccuracies in collected personal information, (3) delete personal information from the website record;
- For *choice*: the firm (1) informs whether personal information will be disclosed to a third party and explains under what conditions, (2) clear choice (asking permission) before disclosing personal information to third party.

Schwaig and colleagues (2006) distinguished multiple levels of Notice, Access and Choice by checking whether a company posts a privacy policy, collects personal information, and mentions:

- For *Notice*: (1) what specific personal information is collected, (2) how the site may use information for internal purposes, (3) whether the site discloses its practice of sharing information with third parties. Notice is "Partial" if at least one of the elements is mentioned, and is "Full", if all the elements are mentioned;
- For *Access*: procedures for the consumer to (1) review information, (2) correct inaccuracies, or (3) remove information. Access is "Partial" if at least one of the elements is mentioned, and is "Full", if all the elements are mentioned;
- For *Choice*: whether the company explicitly asks permission to (1) send personal information to a third party (2) contact the customer for purposes unrelated to the primary relationship. Choice is "Modified" if at least one of the elements is mentioned, and is "Full", if both the elements are mentioned.

In conclusion, the analysis of the two variables operationalization brings out 4 recurring dimensions. Basically, in most of privacy research Transparency/Control mean knowing about/having power over:

- Whether data is collected and what type can be collected;
- How data is used;
- Whether data is shared and for what purpose;
- What specific information has been collected.

Interestingly, the 4 recurring items directly address three of the four dimensions of the Concerns for Information Privacy developed by Smith et al. (1996): Collection, Unauthorized secondary use (internal and external) and Errors. Also, the fourth item perfectly matches the definition of the *Access* Fair Information Practice. The effects of transparency and control on privacy concerns can be declined into the satisfaction of 4 needs whose addressment generates or mitigates different dimensions of privacy concerns.

Note: The fourth dimension of CFIP, Improper Access, would be addressed by the fourth principle of Fair Information Practices (Security) which has been ignored because out of the scope of this research.

CFIP	Need	
	Transparency about	**Control over**
Collection: concern that extensive amounts of personally identifiable data are being collected and stored in databases	Whether data us collected What type of data is collected	
Unauthorized secondary use (internal): concern that information is collected for one purpose but is used for an additional purpose inside the collecting organization	How data is used	
Unauthorized secondary use (external): concern that information is collected for one purpose but is used for an additional purpose inside the collecting organization	Whether data is shared Why data is shared With whom data is shared	
Error: concern that protections against deliberate and accidental errors in personal data are inadequate	What specific information has been collected	

Table 2: Privacy concerns and dimensions of Transparency and Control

2.3 Privacy drivers of consumers behaviour

Transparency

Apparently, privacy concerns and importance of privacy policy are positively associated with importance of information transparency at consumers' eyes. In turn, people for whom transparency is important are less willing to provide their information online in order to receive personalized services or personalized advertising (Awad, et al., 2006). Awad and Krishnan (2006) suggested managers to focus the communication of their firms toward consumers "more willing to partake in online personalization", as the ones "who value transparency features are also less likely to participate in personalized offerings". This conclusion is based on the speculation that this group of consumers is just a segment of privacy fundamentalists not willing to receive personalized offering, no matter the level of transparency and the fairness of data collection procedures. However, that assumption may not hold true anymore, as transparency gets more and more important for consumers and even for authorities. Because of GDPR, there will not be the option of focusing on less privacy sensitive customers. Instead, transparency is going to be mandatorily pursued, at least in Europe. What is more, information transparency may soon become a must have in the market, and not merely an attribute for a limited segment (Trabucchi, et al., 2019).

Another limitation of Awad and Krishnan's research (2006) is that it studies how much customers value and desire transparency, and not its final effect once it is provided. This gap has been investigated by Trabucchi and colleagues (2019): their experiment analysed the effect of business model transparency on willingness to use a digital service for users with a varying level of Privacy Attitude (i.e., the attention paid to how the service provider gathers and use data). Apparently, business model Transparency does not generally affect the willingness to use a service, and neither does Privacy Attitude, in accordance with the Privacy Paradox theory. However, a transparent business model turns out to have a positive effect on willingness to use a service when Privacy Attitude is high, while the opposite cannot be affirmed for the alternative case with a non-transparent model (i.e., opaque).

Moreover, the structure of the experiment enabled to observe the reaction to the shift from a transparent model to an opaque one, and vice versa: changing the business model leads to changes in the Willingness to use the digital service, which decreases when moving from Transparent to Opaque, and increases moving from Opaque to Transparent. Even if transparency does not generally affect behaviour, willingness to adopt a service changes when customers become aware of the existence of a transparent option. If interpreted within the

framework of the Kano model (Berger, 1993), this result has important managerial implications: if adopted by an increasing number of firms, transparency might soon become a must have in the market of digital services. This warning sign, combined with the transformation of transparency into law implemented by the GDPR, visibly increases the role of transparency in the future years.

Privacy policies

Privacy policies are a widespread tool used by firms to inform their customers about their information practices, hence they are the typical mean to provide transparency and increase the perception of data control to those whose data is treated. In fact, privacy policy statements have been analysed to evaluate firm's transparency (Martin, et al., 2017).

Privacy policies effectiveness, described as "the extent to which a consumer believes that the privacy policy notice posted online is able to provide accurate and reliable information about the firm's information privacy practices", (Xu, et al., 2011) is a widely studied construct in the privacy domain (Chang, et al., 2018; Wua, et al., 2012; Nemati, et al., 2009; Zhang, et al., 2019; Xu, et al., 2011).

Privacy policy effectiveness has been found to increase privacy control and decrease privacy risk, mitigate privacy concerns and increase trust (Chang, et al., 2018; Xu, et al., 2011; Wua, et al., 2012). Besides, just reading privacy policy statements increases trust and decreases privacy risks (Nemati, et al., 2009), and their readability reduces the social distance between firms and customers, thus increasing trust and willingness to disclose personal information (Zhang, et al., 2019).

However, the spread of numerous business models built upon the exploitation of value from data and the increasing complexity of data treatments caused the adequacy and the usefulness of privacy policy to be questioned. Apparently, every website user visits at least 1,354 unique websites and that the average cost for the time they spend is $4.48 per hour (if a privacy policy is read at home) or $35.86 per hour (if the Privacy Policy should be read in office). Thus, believing that users would ever be capable to read every single privacy policy might be unrealistic, because of the length of such documents, the time that a user needs to spend and the legal language these policies are written in (McDonald, et al., 2008). According to a recent survey (Deloitte, 2017), only 9 percent of online customers read privacy statements before accepting legal terms and conditions. The problems embedded in privacy policies have been summarized in 8 privacy policy hurdles that undermine their readability and effectiveness:

language complexity, vagueness of terms, wall of text, excessive length, lack of audience-tailoring, bad timing, lack of familiarity and scattered information (Rossi, et al., 2020).

Control

The most adopted framework to study the effect of Perceived Data Control on consumers behaviour in the information privacy domain is the control-risk framework, which adopts the calculus perspective of privacy to incorporate the interplay between risk and control (Dinev, et al., 2006; Dinev, et al., 2013; Libaque-Sáenz, et al., 2020; Chang, et al., 2018). The risk-control literature posits a positive relationship between control perceptions and optimistic bias (Harris, 1995). The greater the perception of control over the outcome, the more positive the expectation about the event (Klein, et al., 2002). This implies that individuals will assess the associated risk as less serious and are more willing to take risk (Brandimarte, et al., 2012). As a consequence, perceived data control decreases perceived information risks (Das, et al., 2001; Li, 2001; Libaque-Sáenz, et al., 2016; Libaque-Sáenz, et al., 2020).

Generally, PDC has been proven as a successful mitigator of privacy concern: people tend to be less concerned about information practices when they feel to have a certain degree of control over them (Dinev, et al., 2006; Dinev, et al., 2013; Chang, et al., 2018; Xu, et al., 2012; Culnan, et al., 1999; Culnan, et al., 2003; Phelps, et al., 2000; Milne, et al., 1999;Xu, 2007; Dinev, et al., 2004), both directly and through the decrease of PIR (Milne, et al., 2004).

Finally, this means that perceived data control has a positive effect on behavioural intention, that is generally offset by privacy concerns. That includes a higher propensity to adopt mobile apps (Libaque-Sáenz, et al., 2020; Dinev, et al., 2013; Dinev, et al., 2006), a better propensity to personalized and targeted advertisements (Tucker, 2014) and a higher willingness to disclose personal information and purchase intention (Bornschein, et al., 2020).

Fair Information Practices

Together, transparency and control are advocated by FIPs, whose adoption effects have been typically studied by evaluating how their presence in the firms' privacy policy statement affected privacy policy effectiveness. their adoption of Fair Information Practices (Schwaig, et al., 2006), and the effects of each of the FIPs dimensions (Notice, Choice, Access, Security) on privacy policy effectiveness have been studied to understand how the adoption of FIPs affect consumers behaviour (Chang, et al., 2018, Nemati, et al., 2009, Wua, et al., 2012).

There is not a shared consensus about the role of FIPs on privacy policy effectiveness: Chang and colleagues (2018) report that the presence of the Notice, Access and Security dimension in the privacy policy does increase its effectiveness, while the same cannot be affirmed for Choice. On the contrary Nemati and colleagues (2009) failed to find a significant relationship between each of the dimensions and privacy policy effectiveness. Finally, other studies reported that the access and security dimension in the privacy policy decreases privacy concern, while notice, access and security increase customers' trust in the firm (Wua, et al., 2012).

Transparency and control interaction

Researches about the interaction of transparency and control have brought other interesting results: the effects of transparency and control have been investigated by Martin and colleagues (2017), who examined how they mediated the relationship between data use vulnerability (i.e., a customer's perception of their susceptibility to being harmed as a result of various uses of their personal data) and possible consumer reactive behaviour and firm performances. At both firm and customer levels, data vulnerability generates negative outcomes for firms, including negative abnormal stock returns and damaging customer behaviours (i.e., falsifying information, spreading negative WOM, and engaging in switching behaviours). The interaction of data transparency and customer control practices has a strong role in suppressing these detrimental effects: even if the two constructs independently mitigate the effect of high data vulnerability on emotional mechanisms (which in turn causes damaging customer behaviour), their combination also suppresses the negative effect of vulnerability on trust and performances on the share market. Moreover, when provided with high transparency but low control, customers perceive more violation and lower trust across all studies, so knowledge alone has mixed effects on vulnerability (Martin, et al., 2017). Therefore, the analysis of Transparency separated by Control may generate misleading results.

Similar results have been reported also in the cookies domain (Bornschein, et al., 2020). The effects of two typologies of cookie notices were analysed: (1) "information-only" notice, with which website limit themselves to inform visitors about the usage of cookies, and (2) "mixed-consent" notice, where visitors have the option to disable at least some of the active cookies. Apparently, notice increases risk perception, while choice increases power perception, which in turn decreases risk perceptions. Higher risk decreases consumers affect and behavioural intentions, whereas higher power improves affect and increases purchase intention. Again, transparency without control may have negative effect on consumers.

2.4 Summary

In conclusion, Information Transparency and Data Perceived Control are two major mediators of privacy concerns: they have been analysed and advocated for through different conceptualizations by both researchers and regulators, and their relationship with privacy concerns can be measured in terms of addressment of 3 of the 4 Concerns for Information Privacy: Collection, Unauthorized Secondary Use (internal and external) and Errors.

The implementation of Transparency and Control to mitigate privacy concerns should interest firms leveraging data driven business model, for which data and personal information are a core asset. To guarantee the sustainability of these business model and continue to thrive in an always more competitive market, two-sided platforms could implement transparency and Control in their value proposition as a strategy to reduce privacy concern and thus suppress their negative effects on behavioural intention.

3. Research Design

This research is aimed at evaluating how firms that collect and leverage user generated data are addressing the rising users' privacy concerns.

Several cases of firms for which data fills a relevant role in the business model have been analysed, in order to assess the current market behaviour and identify alternative strategies in addressing the right to privacy. The multiple case studies analysis (Yin, 2013) allows for replication logic and has been pursued by previous studies to deal with the early stages of research on a topic (Amit, et al., 2001; Galunic, et al., 2001). In fact, it has been already used in business model research for studying data-based business models (Trabucchi, et al., 2019; Buganza, et al., 2019; Trabucchi, et al., 2017a; Trabucchi, et al., 2017b).

Similar analysis have already been carried out in the privacy domain as well, in particular to evaluate the adoption of Fair Information Practices and its effects:

- Bornschein and colleagues (2020) screened the 10.000 most visited websites and evaluated the style of the cookie notices to assess the level of adherence to GDPR and the effect of Notice and Choice on consumers behaviour;
- Schwaig and colleagues (2006) analysed the privacy policies of the Fortune 500 to assess the degree of implementation of the Fair Information Practices;
- Nemati and colleagues (2009) analysed the privacy policies of 80 e-commerce websites to evaluate how the implementation of FIPs affected trust and perceived risk of visitors.

The following research has been designed to answer the following research questions:

1. Are firms leveraging data driven business models implementing Transparency and Control in their value proposition to address rising privacy concerns?
2. What are the current levels of Transparency and Control offered by the most relevant players in the market?
3. What dimensions of Privacy Concerns are addressed the most through Transparency and Control?
4. Are there any industry-related trends regarding Transparency, Control, and how they are used to address Privacy Concerns?
5. Are there any recurring strategies regarding the addressment of Privacy Concerns among firms leveraging data driven business models?

3.1 Assessment model

In order to analyse how firms are currently employing transparency and control in their value proposition to address privacy concerns, an assessment model has been designed.

Its description will answer three questions:

- Domain: Where is the analysis set?
- Subject: What has been measured?
- Level: How has it been measured?

Research domain: The mobile app market

The screening has been set in the mobile app market for several reasons:

- It is a very big and wide market, which represents a relevant portion of the population, as smartphones diffusion is very high and still increasing;
- Smartphone technology allows for extensive and pervasive collection of data;
- Smartphones are very personal belongings that act nowadays as the first channel of connection between the users and Internet, hence they are tool through which a massive amount information is generated.

For these reasons, the mobile app market flourishes with an ever-increasing number of players whose business model relies on data (the subjects of this research) and is usable as a representative sample of the subject of the research.

Research subject: Transparency and Control levels

The operationalization of Transparency and Control is grounded on the literature review presented in the previous chapter, which identified a direct association between 4 recurring dimensions of the definition of the two constructs and 3 of the 4 Concerns for Information Privacy. Both Transparency and Control have been measured across 4 measurement dimensions: Collection, Usage, Sharing and Access.

The Transparency level has been measured as the degree with which the firm informs is customer about:

- *Collection*: whether data is collected and what type of data is collected;
- *Usage*: how data is used;
- *Sharing*: whether data is shared, why data is shared and with whom data is shared;
- *Access*: what specific information has been collected.

The Control level has been measured as the degree with which the firm allows the customer to control:

- *Collection*: whether data is collected and what type of data is collected;
- *Usage*: how data is used;
- *Sharing*: whether data is shared, why data is shared and with whom data is shared;
- *Access*: what specific information has been collected.

The meaning of the four areas and their role in connecting transparency, control and privacy concerns is summarized in the table below.

Dimensions of Privacy Concerns	**Measurement dimensions**	**Transparency** **Know about:**	**Control** **Power over:**
Collection	Collection	Whether data is collected What type of data is collected	
Unauthorized secondary use (internal)	Usage	How data is used by the collecting organization	
Unauthorized secondary use (internal)	Sharing	Whether data is shared Why data is shared With whom data is shared	
Error	Access	What specific information has been collected	

Table 3: Areas of measurement of Transparency and Control

Note: the fourth dimension "Access" extends the meaning of the "Error" privacy concern dimension and is based on the Access principle of the FIPs. The principle has been chosen as area of measurement over the privacy concern because it has a higher resemblance to the operationalizations of Transparency and Control used in literature, is appliable to both constructs and it also addresses the privacy concern (offering transparency or control over the specific data can be way to reassure users of the absence of errors in the information stored about them).

Research level: User Experience

Until now, previous research evaluating the Transparency and Control level of the market used privacy policy analysis to check for the implementation of Fair Information Practices (Nemati, et al., 2009; Schwaig, et al., 2006; Wua, et al., 2012; Chang, et al., 2018). In fact, privacy policies analysis has been used also in strategy research, to investigate current strategies of data driven business models (Buganza, et al., 2019; Trabucchi, et al., 2017a).

Unfortunately, privacy policies are proving themselves a poor instrument to be transparent and empower users (McDonald, et al., 2008; Rossi, et al., 2020) and are frequently ignored by consumers of digital services (Deloitte, 2017). Hence, with the objective of investigating the true accessibility of the information disclosed or the power granted to consumers, this research analyses the degree of transparency and control provided directly in the user experience, rather than described in the privacy policies.

The presence of transparency and control in the user experience has been already explored: the implementation of Notice and Choice in websites has been evaluated by assessing the visibility of their cookies notice and the number of options they allowed (Bornschein, et al., 2020). Ataei and colleagues (2018b) designed a set of user interface (UI) controls for fine-grained management of location privacy settings based on privacy theory (Westin, 1967), privacy by design principles and general UI design principles, and then tested its usability and effectiveness in managing privacy setting with a set of experiments. Ataei and colleagues (2018a) have drawn up a set of guidelines for UX developers who need to address privacy concerns and adhere to GDPR in the realization of app offering location-based services.

Each of the areas of measurement presented in the previous paragraph has been evaluated through a direct usage of each of the unit of analysis, and the presence of information or controls addressing the associated concern has been collected.

3.2 Data Collection

Sampling strategy

In order to apply the assessment model in the smartphone applications domain, the Android App Marketplace (https://play.google.com/store/apps) has been chosen as the source of the sample source. The first version of the sample has been populated with the 100 most downloaded applications, in order to obtain a heterogenous group of popular apps (each of the unit has been downloaded at least 500 million times). The ranking that has been reported reflects the one visible on androidrank.org (AND21).

Every app has been downloaded, initialized, and tested through two testing devices (Pixel 5 and OnePlus 5) to assess the level of Transparency and Control. The final sample excluded:

- 11 applications not accessible to non-Samsung smartphones (Samsung Gallery, Samsung Email, Samsung Push Service, Briefing, Samsung Calendar, Samsung Calculator, Device Care, Samsung ONE UI Home, Samsung My files, Secure Folder, Samsung Experience Service, Samsung Voice Recorder);
- 13 utility plugins that, even if downloadable as apps in the Play Store, do not have a graphical user interface to be used from the smartphone (Google Play Services, Android Accessibility Suite, Google Text-to-speech, Gboard, Android System WebView, Android Auto, Carrier Service, Cloud Print, Samsung Print Service Plugin, Google Play Services for AR, ANT Radio Service, ANT+ Plugins Service, HP Print Service Plugin);
- 3 applications not available for download (Google Play Music, Currents, YouTube Go);
- 2 application replicating other analysed apps (Facebook Lite, Messenger Lite).

The final sample contained 71 apps. The privacy policies of all of them have been reviewed to verify that they performed at least one activity of data treatment, such as collection, usage and sharing.

Variables measurement

In order to assess the level of transparency and control for each unit of the sample the 4 measurement dimensions have been declined, for both Transparency and Control, in a set of "macro-capabilities" that an app can offer its users to provide Transparency and control.

Measurement dimension	**Transparency**	**Control**
Collection	The user is informed that data is collected. The user is informed of what types of data are collected. The user is informed about how data is collected.	The user can decide whether data are collected. The user can decide what types of data are collected

Usage	The user is informed of how the data collected by the app are used by the app itself.	The user can decide for what purposes the data collected by the app can be used by the app itself.
Sharing	The user is informed of whether data are shared with third parties, who are them, how they use them and what data is being shared.	The user can decide whether the app can share data with third parties, who to share it with, for what reasons and what to share
Access	The user can see/download the data that has been collected.	The user can correct/delete the collected data.

Table 4: Application of the areas of measurement to the assessment model

Note: the sharing dimensions captures activities of bi-directional sharing, meaning that whatever information or control referring to the exchange of data between the app and a third party is mapped in this dimension. That accounts for cases in which the app collects data and share them with partners, and for cases in which third parties collect data about the individual and then share it with the analysed app. This means that this kind of information and control are referred only to the "Sharing" dimension, and not to the "Usage" one, that is associated only to data treatment performed by the collecting app.

For every unit of the sample:

- The presentation page in the Play Store has been read;
- The app has been initialized (all the steps required before being able to use the app have been performed);
- The settings menu has been explored thoroughly.

Every information and control which offered one or more of the macro-capabilities previously described has been noted and mapped to the corresponding dimension. Then, the total number of information or options for each dimension for both Transparency and Control has been computed.

Information and options addressing different dimensions, but the same data type or data treatment have been grouped together to improve the readability of the results. Also, transparency and controls features referring to the same data type or data treatment have been grouped together.

An example is here reported:

Table 5: Example: Youtube analysis

APP	TRANSPARENCY/CONTROL FEATURES ADDRESSING SPECIFIC DATA TREATMENT OVER SPECIFIC DATA TYPES	TRANSPARENCY				CONTROL			
		COLLECTION	USAGE	SHARING	ACCESS	COLLECTION	USAGE	SHARING	ACCESS
YouTube	You can allow YouTube to collect your search history and use it to personalize your experience. You can see it, together with the details of each specific search, and delete it completely or partially.	x	x		x	x			x
	You are informed that you can allow YouTube to collect the history of what you watch and use it to personalize your experience. You can see it, together with the details of each specific activity, and delete it completely or partially.	x	x		x	x			x
	You can see the type of data YouTube collects and download all of them.	x			x				
	You can set the periodic elimination of the history of your activities on YouTube.								x
	You can see the list of third-party apps connected to your account. You can revoke the connection.			x				x	
	You are informed that other YouTube Apps share data about you with YouTube to personalize your experience.			x					
		3	2	2	3	2	0	1	3

Using the first row as example, the subject here is the data about the videos the user searches with the app. The measurement dimensions addressed are:

- For transparency
    - Collection, because it is explained what data is collected (the videos the user searches with the search bar);
    - Usage, because it is explained why data are collected with different examples (personalize ads, suggest content to watch, send notifications about new videos the user may like);
    - Access, because the user can access and see the history of the searches together with their details.
- For Control
    - Collection, because the user can stop the collection of that specific type of data;
    - Access, because the user can delete some searches or clear completely the history.

The output of the analysis for the app is that it provides:

- 11 information about data treatments
    - Collection (3): a dedicated message for the searches and the videos watched explicitly saying that they are collected and a page of download listing all the types of data collected;
    - Usage (2): a dedicate explanation of why the searches and the videos watched are collected and how they are used;
    - Sharing (2): the possibilty to see the identity of third-party apps connected to your account and the warning that some data are shared to other applications of the YouTube family;
    - Access (3): the possibility to review the search and watch history and to download all the collected data.
- 6 options to manage data treatment:
    - Collection (2): the possibility to allow/forbid the collection of 2 specific types of data;
    - Sharing (1): the possibility to cancel the connection with specific third party apps;
    - Access (3): the possibility to delete some searches or watched videos or to set their periodic elimination (which has been counted once because when enabled it applies to both types of data).

Additional rules

The following rules have been adopted to guarantee the maximum consistency of the data.

1. The access requests to the device (contacts, storage, microphone, camera, etc…) has not been counted as a feature of control, because they are imposed by the Android Operating System, and thus are not a choice of the app's value proposition.

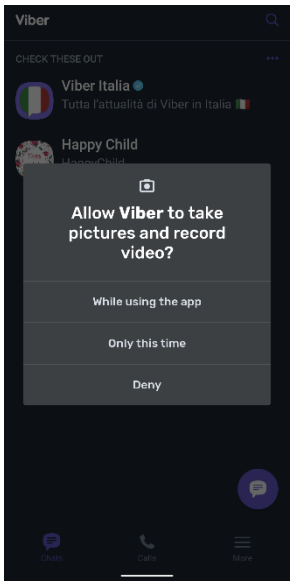

Figure 3: Android UX for granting access to the smartphone's camera

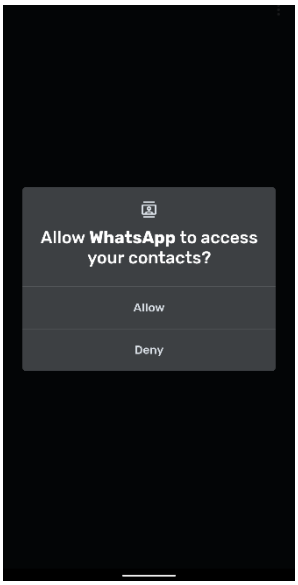

Figure 1: Android UX for granting access to the device's phonebook

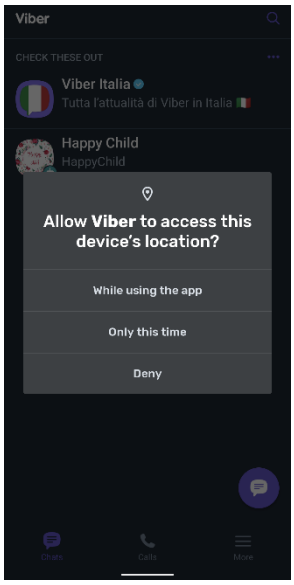

Figure 2: Android UX for granting access to the device's location

However:

- The presence of a customized message dedicated to warning the user before the request (which is prompted by the app but handled by the OS) explaining the reason behind it was considered a transparency feature;

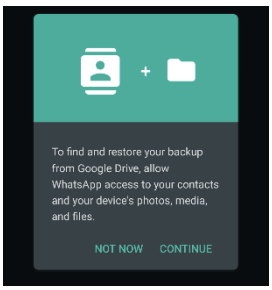

Figure 4: WhatsApp warning for the request to access contacts and storage

- The possibility to manually handle the permission (revoking it or re-prompting the OS to ask for it) from the app settings was considered a control feature.

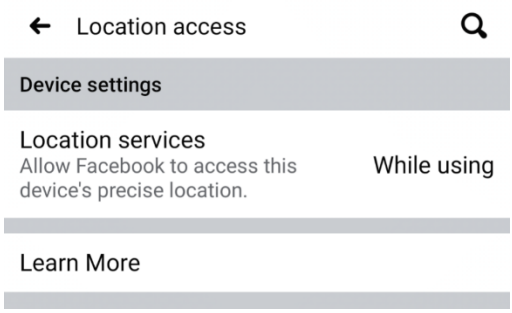

Figure 5: Facebook's option to customize the access to the device's location

2. Many apps offered by Google does not offer a dedicated privacy menu. Instead, the data coming from their utilization converges in the Google Account, from where it is possible manage different privacy and data settings. Here, it is typically not possible to manage data per app, hence:

- Google apps have been analysed individually according to what transparency and control features they offer regarding exclusively the data generated and used by them (e.g. YouTube and Google Maps have a list of settings similar to the one offered for the Google Account but specific for their data of interest)
- The Google account privacy management settings have been reviewed in the Google app (#7)

The same criteria has been applied to Messenger and Facebook, where the first is manageable mainly with the settings of the first.

4. Findings

4.1 Summary

Data regarding each single case are reported in Appendix A. A summary is presented below.

RANKING	APP	TRANSPARENCY				CONTROL			
		Collection	Usage	Sharing	Access	Collection	Usage	Sharing	Access
1	GOOGLE PLAY SERVICES	Not an app with a proper UI							
2	WHATSAPP	3	2	0	1	0	0	0	1
3	FACEBOOK	12	6	4	8	4	2	3	6
4	YOUTUBE	3	2	2	3	2	0	1	3
5	GOOGLE PHOTOS	3	2	1	0	0	1	0	0
6	GOOGLE CHROME	7	1	5	1	10	0	9	2
7	GOOGLE	6	5	1	5	6	1	1	5
8	GOOGLE MAPS	4	2	1	2	2	1	1	1
9	GMAIL	0	0	0	0	0	0	0	0
10	GOOGLE DRIVE	0	0	0	0	0	0	0	0
11	GOOGLE PLAY MUSIC	Replaced by YouTube Music (#97)							
12	ANDROID ACCESSIBILITY SUITE	Not an app with a proper UI							
13	GOOGLE TEXT-TO-SPEECH	Not an app with a proper UI							
14	GOOGLE TV	0	0	0	0	0	0	0	0
15	INSTAGRAM	6	2	3	5	1	0	1	1
16	MESSENGER	2	2	0	0	2	0	0	0
17	SUBWAY SURFERS	2	1	1	0	1	0	0	0
18	TIKTOK	6	4	2	2	2	1	1	2
19	CANDY CRUSH SAGA	0	0	2	0	0	0	0	0
20	SNAPCHAT	8	3	4	4	3	1	3	3
21	TWITTER	6	5	3	2	3	2	3	2
22	FACEBOOK LITE	Repetition of Facebook							
23	SHAREIT	6	6	0	1	2	0	0	2
24	GOOGLE PLAY GAMES	2	1	0	1	0	0	0	3
25	SKYPE	3	2	1	0	2	0	1	1

RANKING	APP	TRANSPARENCY				CONTROL			
		Collection	Usage	Sharing	Access	Collection	Usage	Sharing	Access
26	**NETFLIX**	2	2	0	1	0	1	0	0
27	**GBOARD**	Not an app with a proper UI							
28	**GOOGLE DUO**	4	0	0	0	2	0	0	1
29	**CURRENTS**	Not available to standard accounts (only Business)							
30	**MICROSOFT WORD**	4	2	1	1	1	0	0	0
31	**HANGOUTS**	3	3	0	0	2	1	0	0
32	**ANDROID SYSTEM WEBVIEW**	Not an app with a proper UI							
33	**MESSAGES**	4	3	2	0	0	2	1	0
34	**SAMSUNG INTERNET BROWSER**	5	2	1	2	6	0	5	2
35	**MICROSOFT EXCEL**	4	2	1	1	1	0	0	0
36	**SAMSUNG GALLERY**	Not available for non-Samsung devices							
37	**GOOGLE STREET VIEW**	0	0	0	0	0	0	0	0
38	**ONEDRIVE**	2	2	0	1	1	0	0	0
39	**DROPBOX**	2	1	0	1	1	0	0	1
40	**GOOGLE PLAY BOOKS**	0	0	0	0	0	0	0	0
41	**MICROSOFT POWERPOINT**	4	2	1	1	1	0	0	0
42	**SAMSUNG EMAIL**	Not available for non-Samsung devices							
43	**GOOGLE CALENDAR**	2	1	1	0	0	0	1	0
44	**ANDROID AUTO**	Not an app with a proper UI							
45	**GOOGLE DOCS**	1	1	0	0	0	0	0	0
46	**GOOGLE NEWS**	0	0	0	0	0	0	0	0
47	**SAMSUNG HEALTH**	4	1	2	1	3	1	2	0
48	**GOOGLE KEEP**	1	1	0	0	0	0	0	0
49	**SAMSUNG PUSH SERVICE**	Not available for non-Samsung devices							
50	**BRIEFING**	Not available for non-Samsung devices							
51	**CARRIER SERVICE**	Not an app with a proper UI							
52	**CLOUD PRINT**	Not an app with a proper UI							
53	**SAMSUNG PRINT SERVICE PLUGIN**	Not an app with a proper UI							

RANKING	APP	TRANSPARENCY				CONTROL			
		Collection	Usage	Sharing	Access	Collection	Usage	Sharing	Access
54	SAMSUNG CALCULATOR	Not available for non-Samsung devices							
55	GOOGLE PLAY SERVICES FOR AR	Not an app with a proper UI							
56	DEVICE CARE	Not available for non-Samsung devices							
57	ANT RADIO SERVICE	Not an app with a proper UI							
58	ANT+PLUGINS SERVICE	Not an app with a proper UI							
59	SAMSUNG ONE UI HOME	Not available for non-Samsung devices							
60	SAMSUNG MY FILES	Not available for non-Samsung devices							
61	SECURE FOLDER	Not available for non-Samsung devices							
62	SASMSUNG EXPERIENCE SERVICE	Not available for non-Samsung devices							
63	SAMSUNG VOICE RECORDER	Not available for non-Samsung devices							
64	GARENA FREE FIRE	1	1	0	0	0	0	0	0
65	CLASH OF CLANS	1	0	1	0	0	0	1	0
66	UC BROWSER	3	0	0	2	1	0	1	3
67	SPOTIFY	0	0	0	0	0	0	0	0
68	MY TALKING TOM	0	0	2	0	0	0	2	0
69	VIBER MESSENGER	14	2	15	1	2	1	11	1
70	TRUECALLER	3	5	1	1	0	1	0	1
71	MY TALKING ANGELA	0	0	2	0	0	0	2	0
72	LINE	3	3	1	0	3	0	1	1
73	WISH	0	0	1	0	0	0	1	1
74	POU	0	1	0	0	0	1	0	0
75	PICSART PHOTO EDITOR	2	1	0	1	1	0	0	2
76	MX PLAYER	3	2	1	1	0	0	0	1
77	HILL CLIMB RACING	1	0	1	0	0	0	1	0
78	LIKEE	1	0	1	0	0	0	1	0
79	TEMPLE RUN 2	1	1	2	0	1	0	1	0
80	UBER - REQUEST A RIDE	1	1	0	0	1	0	0	0
81	GOOGLE TRANSLATE	3	2	0	1	1	0	0	1

RANKING	APP	TRANSPARENCY				CONTROL			
		Collection	Usage	Sharing	Access	Collection	Usage	Sharing	Access
82	**PINTEREST**	6	5	3	0	3	2	3	3
83	**OPERA MINI**	3	1	2	1	4	0	3	3
84	**TELEGRAM**	3	1	2	0	1	0	1	3
85	**B612**	2	0	0	0	1	0	0	1
86	**LUDO KING**	0	0	0	0	0	0	0	0
87	**IMO**	3	2	0	1	2	0	0	1
88	**TEMPLE RUN**	1	1	2	0	1	0	1	0
89	**MESSENGER LITE**	Repetition of Messenger							
90	**ADOBE ACROBAT READER**	2	1	0	0	2	0	0	0
91	**FILES BY GOOGLE**	2	1	0	1	0	0	0	1
92	**SHAZAM**	0	0	0	0	0	0	0	0
93	**MICROSOFT SWIFTKEY KEYBOARD**	3	3	0	0	1	1	0	1
94	**8 BALL POOL**	0	0	1	0	0	0	1	0
95	**HP PRINT SERVICE PLUGIN**	Not an app with a proper UI							
96	**MI FILE MANAGER**	1	0	0	0	0	0	0	1
97	**YUTUBE MUSIC**	7	5	1	4	4	1	1	4
98	**YOUTUBE GO**	Not available on the Play Store anymore							
99	**LINKEDIN**	18	9	7	7	4	5	7	8
100	**ZOOM**	1	1	0	0	1	0	0	0

Table 6: Transparency and Control levels per privacy concern per app

4.2 Sample overview

RANKING	APP	CATEGORY	TRANSPARENCY	CONTROL	$\frac{Transparency}{Control}$
2	**WHATSAPP**	Communication	6	1	6,0
3	**FACEBOOK**	Social	30	15	2,0
4	**YOUTUBE**	Video Players	10	6	1,7
5	**GOOGLE PHOTOS**	Photography	6	1	6,0
6	**GOOGLE CHROME**	Tools	14	21	0,7
7	**GOOGLE**	Tools	17	13	1,3
8	**GOOGLE MAPS**	Travel & Local	9	5	1,8
9	**GMAIL**	Communication	0	0	-
10	**GOOGLE DRIVE**	Productivity	0	0	-
14	**GOOGLE TV**	Video Players	0	0	-
15	**INSTAGRAM**	Social	16	3	5,3
16	**MESSENGER**	Communication	4	2	2,0
17	**SUBWAY SURFERS**	Game	4	1	4,0
18	**TIKTOK**	Social	14	6	2,3
19	**CANDY CRUSH SAGA**	Game	2	0	-
20	**SNAPCHAT**	Social	19	10	1,9
21	**TWITTER**	Social	16	10	1,6
22	**FACEBOOK LITE**	Social			
23	**SHAREIT**	Tools	13	4	3,3
24	**GOOGLE PLAY GAMES**	Enterteinment	4	3	1,3
25	**SKYPE**	Communication	6	4	1,5
26	**NETFLIX**	Enterteinment	5	1	5,0
28	**GOOGLE DUO**	Communication	4	3	1,3
30	**MICROSOFT WORD**	Productivity	8	1	8,0

RANKING	APP	CATEGORY	TRANSPARENCY	CONTROL	$\frac{Transparency}{Control}$
31	**HANGOUTS**	Communication	6	3	2,0
33	**MESSAGES**	Communication	9	3	3,0
34	**SAMSUNG INTERNET BROWSER**	Communication	10	13	0,8
35	**MICROSOFT EXCEL**	Productivity	8	1	8,0
37	**GOOGLE STREET VIEW**	Travel & Local	0	0	-
38	**ONEDRIVE**	Productivity	5	1	5,0
39	**DROPBOX**	Productivity	4	2	2,0
40	**GOOGLE PLAY BOOKS**	Books & Reference	0	0	-
41	**MICROSOFT POWERPOINT**	Productivity	8	1	8,0
43	**GOOGLE CALENDAR**	Productivity	4	1	4,0
45	**GOOGLE DOCS**	Productivity	2	0	-
46	**GOOGLE NEWS**	News & Magazines	0	0	-
47	**SAMSUNG HEALTH**	Health & Fitness	8	6	1,3
48	**GOOGLE KEEP**	Productivity	2	0	-
64	**GARENA FREE FIRE**	Game	2	0	-
65	**CLASH OF CLANS**	Game	2	1	2,0
66	**UC BROWSER**	Communication	5	5	1,0
67	**SPOTIFY**	Music & Audio	0	0	-
68	**MY TALKING TOM**	Game	2	2	1,0
69	**VIBER MESSENGER**	Communication	32	15	2,1
70	**TRUECALLER**	Communication	10	2	5,0
71	**MY TALKING ANGELA**	Game	2	2	1,0
72	**LINE**	Communication	7	5	1,4
73	**WISH**	Shopping	1	2	0,5

RANKING	APP	CATEGORY	TRANSPARENCY	CONTROL	$\frac{Transparency}{Control}$
74	**POU**	Game	1	1	1,0
75	**PICSART PHOTO EDITOR**	Photography	4	3	1,3
76	**MX PLAYER**	Video Players	7	1	7,0
77	**HILL CLIMB RACING**	Game	2	1	2,0
78	**LIKEE**	Video Players	2	1	2,0
79	**TEMPLE RUN 2**	Game	4	2	2,0
80	**UBER - REQUEST A RIDE**	Maps & Navigation	2	1	2,0
81	**GOOGLE TRANSLATE**	Tools	6	2	3,0
82	**PINTEREST**	Lifestyle	14	11	1,3
83	**OPERA MINI**	Communication	7	10	0,7
84	**TELEGRAM**	Communication	6	5	1,2
85	**B612**	Photography	2	2	1,0
86	**LUDO KING**	Game	0	0	-
87	**IMO**	Communication	6	3	2,0
88	**TEMPLE RUN**	Game	4	2	2,0
90	**ADOBE ACROBAT READER**	Productivity	3	2	1,5
91	**FILES BY GOOGLE**	Tools	4	1	4,0
92	**SHAZAM**	Music & Audio	0	0	-
93	**MICROSOFT SWIFTKEY KEYBOARD**	Productivity	6	3	2,0
94	**8 BALL POOL**	Game	1	1	1,0
96	**MI FILE MANAGER**	Tools	1	1	1,0
97	**YUTUBE MUSIC**	Music & Audio	17	10	1,7
98	**YOUTUBE GO**	Video Players			
99	**LINKEDIN**	Business	41	24	1,7

RANKING	APP	CATEGORY	TRANSPARENCY	CONTROL	$\frac{Transparency}{Control}$
100	**ZOOM**	Business	2	1	2,0

Table 7: Transparency and Control levels and Transparency/Control ratio per app

5. Discussion

The analysis of the collected data is divided in two parts.

The first one is a descriptive review of the metrics computed with the data summarized at the end of the previous chapter: the final output of the data collection are the levels of transparency and control for each app, defined as the number of information or options offered to address privacy concerns.

The review answers four questions:

1. Are firms leveraging data driven business models implementing Transparency and Control in their value proposition to address rising privacy concerns?
2. What are the current levels of Transparency and Control offered by the most relevant players in the market?
3. What dimensions of Privacy Concerns are addressed the most through Transparency and Control?
4. Are there any industry-related trends regarding Transparency, Control, and how they are used to address Privacy Concerns?

The second part is a focus on units of the sample providing transparency or control before the actual usage of the app, thus being an example of a proactive approach to the addressment of privacy concerns. The approach is apparently implemented in two non-alternative contexts: The Play Store presentation page or the app initialization, and can follow 3 possible strategies (Information Only, Authorization Heads-Up and Early Control) that will be presented later.

5.1 Descriptive metrics

The descriptive analysis explored the distribution metrics of Transparency and Control levels, aggregated together or grouped by privacy concerns or the app's category. Since there are no comparable benchmarks to appreciate the value of the results, the analysis focused on relative indicators and comparisons among the collected variables (transparency, control, privacy concerns, app category).

Transparency and Control

	Transparency	Control
Average	6,8	3,7
Standard deviation	7,6	5,0
Coefficient of variation	112%	133%
Max	41	24
Min	0	0

Table 8: Descriptive metrics of Transparency and Control levels

Apparently, an application provides in average 6.8 distinct informative messages about data treatment and 3.8 options to manage them. The metrics reported in the table show that Transparency is provided more often than Control: the computation of the ratio between the Transparency and Control levels resulted in 2.54, meaning that for every option to control data treatments that is provided there are at least two distinct informative messages communicated to the users.

Note: The Transparency/Control ratio average is computed by averaging the ratio of the units having at least a level of 1 for both mediators. As a consequence, its value differs from the ratio between average transparency and average control levels.

Secondly, dispersion is very high for both constructs: both standard variations are higher than the average levels. In particular, the coefficients of variation ($\frac{\sigma}{average} * 100$) show how dispersion is generally higher for control.

Finally, Transparency and Control show a certain degree of correlation ($correlation\ index = 0.85$), meaning that apps offering high or low transparency generally offer a similar level of control. Figure 6 displays how the sample is distributed (every point represents an app).

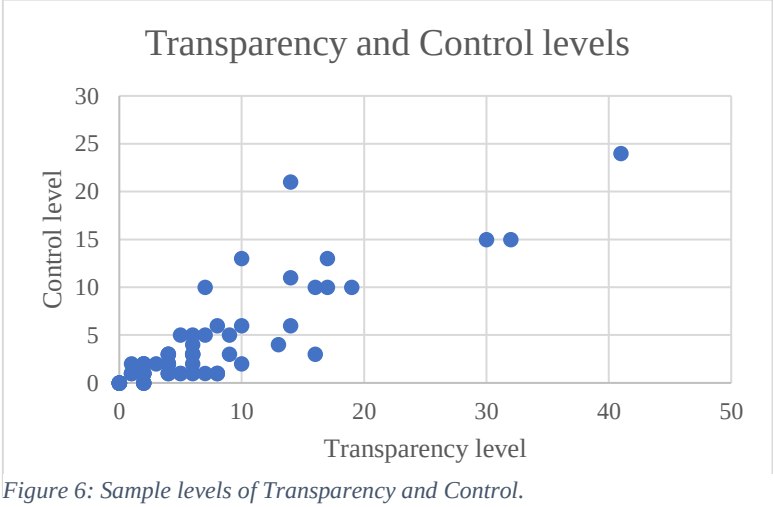

Figure 6: Sample levels of Transparency and Control.

However, some outliers emerge. A contingency table has been redacted by discretizing the levels of transparency and control in two categories:

- **Low**: If the number of information/options provided by the app is lower than the average
- **High**: If the number of information/options provided by the app is higher than the average

Transparency	High	24 (34%)	7 (10%)	17 (24%)
	Low	47 (66%)	44 (62%)	3 (4%)
		71	51 (72%)	20 (28%)
			Low	High
			Control	

Table 9: Contingency table

The majority of the sample (62%) offers less transparency and control of the average, showing a higher density below average for both constructs, and a smaller group (24%) of "fair" apps position themselves above average for both transparency and control levels.

The table highlights the presence of two clusters that stand out:

- 7 apps (10%) are more transparent than the average but offer less control. They are Instagram, Microsoft Word, Messages, Microsoft Excel, Microsoft PowerPoint, Truecaller, MX Player
- 3 apps (4%) offer more control than average but are less transparent than the rest of the sample. They are Skype, UC Browser and Telegram. Nevertheless, for all of them the number of information communicated is at least equal to the number of options provided.

Privacy concerns

The analysis of how Transparency and Control are used to address different privacy concerns is based on the average levels of Transparency and Control for each of the 4 areas of measurement the 4 area of measurement (Collection, Usage, Sharing and Access) offered by every unit.

	Collection	Usage	Sharing	Access
Transparency	2.96	1.66	1.20	0.92
Control	1.30	0.37	1.01	1.03
Total	4.25	2.03	2.21	1.94

Table 10: Addressment levels of privacy concerns per construct

The relevance of each concern dimension has been computed as the ratio between the number of times such concern has been addressed through transparency or control feature and the sum of transparency and control levels of each app (Figure 7). The most addressed concern is typically the one referring to the "Collection" dimension, followed by Sharing, Usage and Access. While collection is notably the most relevant, the others are generally addressed in a similar measure.

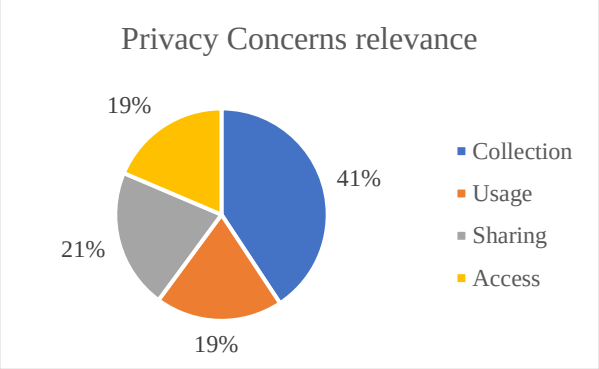

Figure 7: Average percentage of privacy concern addressment

However, the drill down of the data per mediator offers additional insights to evaluate how transparency and control are used to address privacy concerns. In particular, the "Usage"

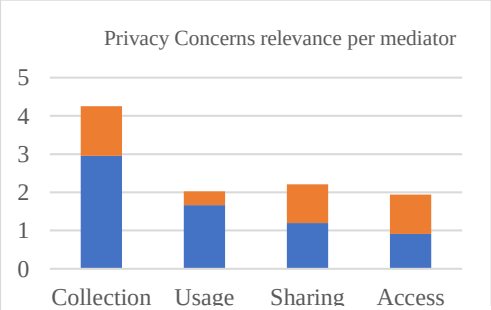

Figure 9: Level of addressment of privacy concerns per contruct (piled columns)

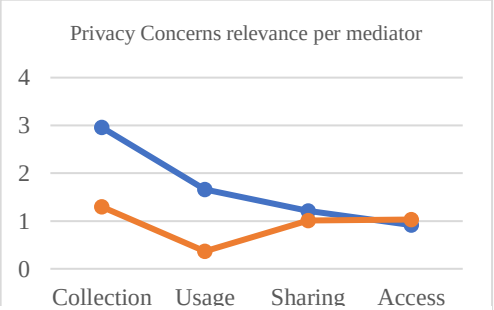

Figure 8: Level of addressment od privacy concerns per construct (lines)

privacy concern presents an odd behaviour: it is the one offering the least control (0.37), while being the second one more addressed concern through transparency. In fact, it is the concern with the highest ratio transparency/control (2.74), so it is the one with the biggest disequilibrium between information and power. However, it must be noted that this gap is probably enhanced by the dominance of collection options over usage ones: since it is impossible to analyse and exploit data when they are not available, the possibility to decide about collection makes usage options unnecessary.

The ratio analysis highlights how for both sharing and access the relevancy of transparency over control is almost zeroed (in both cases, the ratio is close to 1):

- For Sharing, a possible interpretation could be that the sharing concerns receive particular attention since they involve third parties and thus there is a higher necessity to provide power to users to reassure them when sharing practices are performed.
- For access, it means that the possibility to see the collected data (exclusively transparency feature) almost balances itself with the possibility to eliminate them without seeing them (exclusively control feature). Furthermore, the remaining feature addressing the Access concern, which is the possibility to modify data, is necessarily a mean to provide both transparency and control, hence it participates to keeping the transparency/control ratio close to 1.

Note: as for the computation of the average transparency/control ratio, the ratios per privacy concerns have been computed only for the apps offering at least one information/option for each concern. For this reason, the values reported in Figure 10 differ from the ratio between the ones in table 10.

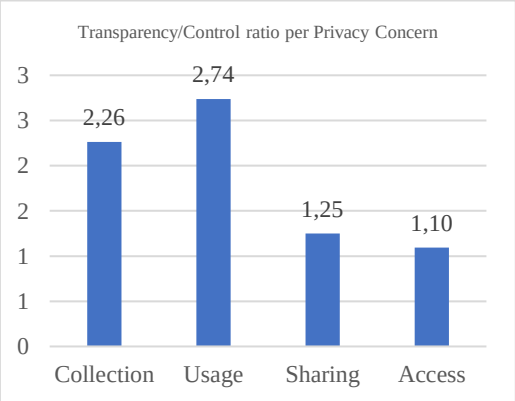

Figure 10: Transparency/Control ratio per privacy concern

Industry analysis

The category of each of the units has been used to group them and look for industry-related trends regarding the level of transparency and control and their relationship. Only categories containing at least 5 units have been considered, their details are reported below.

Category	Number of apps	Apps
Communication	15	WhatsApp, Gmail, Messenger, Skype, Google Duo, Hangouts, Messages, Samsung Internet Browser, UC Browser, Viber Messenger, Truecaller, LINE, Opera Mini, Telegram, imo.
Game	12	Subway Surfers, Candy Cursh Saga, Garena Free Fire, Clash of Clans, My Talking Tom, My Talking Angela, Pou, Hill Climb Racing, Temple Run 2, Ludo King, Temple Run, 8 Ball Pool.
Productivity	11	Google Drive, Microsoft Word, Microsoft Excel, OneDrive, Dropbox, Microsoft PowerPoint, Google Calendar, Google Docs, Google Keep, Adobe Acrobat Reader, Microsoft SwiftKey Keyboard.
Tools	6	Google Chrome, Google, SHAREit, Google Translate, Files by Google, Mi File Manager.
Social	5	Facebook, Instagram, TikTok, Snapchat, Twitter.

Table 11: Categories considered in the industry analysis and their population.

For both transparency and control, the Social and Communication industries clearly stand out from the others, and this is not surprising: apps belonging to these categories heavily leverage data collection and analysis, and in the past years have been under the scrutiny of public opinion and regulators. This pressure probably drives them to rely more on transparency and control levers to mitigate privacy concerns and avoid their effects on behavioural intention. In fact, the willingness to use digital services and to disclose personal information are two relevant drivers of revenues for apps of these two categories, since they intensely rely on the analysis of the data of their users to improve advertisement messages. In particular, Social apps offer a level of transparency and control that nearly doubles average levels (+95% and +85%).

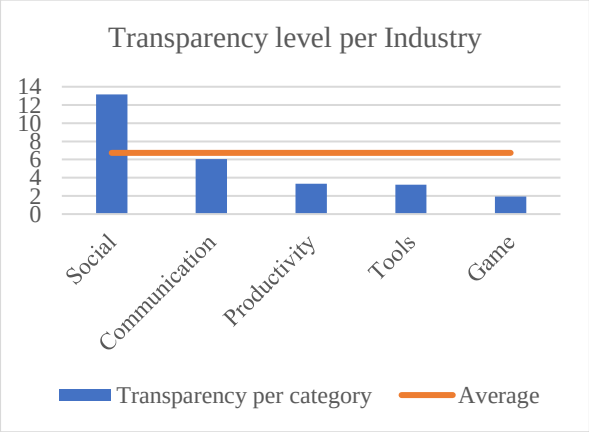

Figure 12: Transparency level per industry

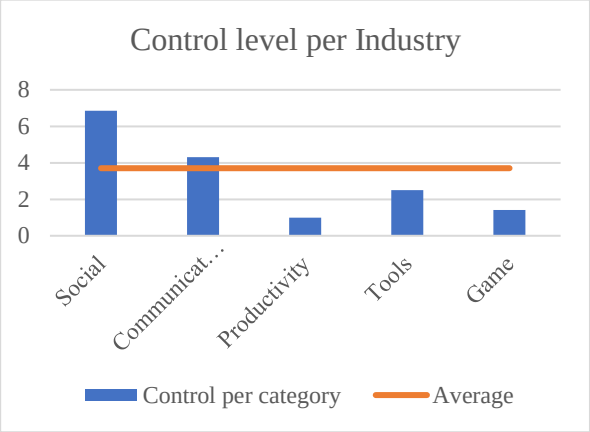

Figure 11: Control level per industry

The analysis of the ratio between transparency and control across category shows that productivity apps have a notably higher disequilibrium between information and power. A possible reason might be that this type of app usually perform less relevant data treatments, follow alternative business models and thus are less pressured to offer control to their user to mitigate privacy concerns. Interestingly, Social apps do not appear to use a higher reliance on control features to address privacy concerns than average.

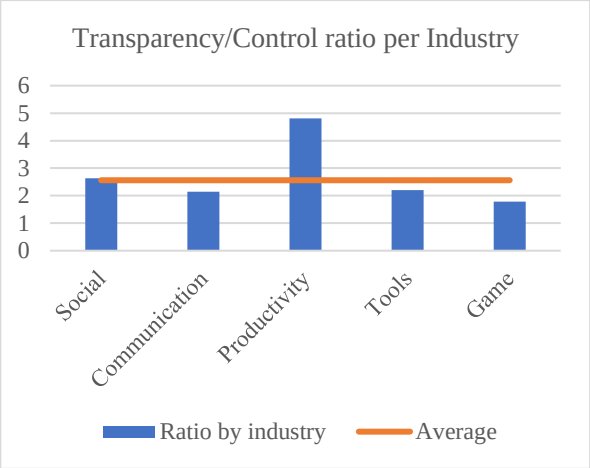

Figure 13: Transparency/Control ratio per industry

5.2 Proactive Transparency and Control

The second part of the analysis is a focus on those apps proposing a proactive approach to Transparency and Control, meaning that they offer one or both before the users start to actually use the app. This approach is also consistent with some definitions of transparency (Trabucchi

et al, 2019; Culnan and Armstrong, 1999) which specifically referred to a communication of data practices in the service presentation.

The insights generated by this analysis are based on a subset of the information collected and displayed in the Findings and in the Appendix A. In particular, for every unit of the sample the transparency and control features that have been considered are the ones provided:

- In the Play Store page, as part of the presentation of the app publicly available before download.
- In the initialization of the app, (i.e., the series of messages and configurations the user has to go through before actually being able to use the service).

Interestingly, 3 distinct but not exclusive strategies emerged:

- **Information Only**: the user is informed about data practices, but without being able to immediately have control over them.
- **Authorization heads-up**: the user receives informative messages that pre-alert him of what mandatory or optional permissions the app needs to work properly/at best and why.
- **Early control:** the user can manage data options during the service initialization.

The information/options are still grouped by data treatment, as in the previous chapter, but in this case each of them have been mapped according to:

- The channel(s) used: Play Store or Service Activation.
- The strategy(ies) adopted: Information Only, Authorization Heads-up or Early Control.

Note: in both cases, the options are not excludable. An app may use both the Play Store page and the service activation to behave proactively and can follow all the 3 strategies. For example, it may offer "Information Only" for a type of data treatment, "Early Control" for another one and "Authorization heads-up" before requesting particular permissions.

Every app has been assigned to one or more channels/strategies according to whether it had at least one proactivity feature for each of them.

The Truecaller case is an example of an app following all the strategies and using both the channels to behave proactively.

Table 12: Example: Truecaller's analysis

APP	TRANSPARENCY OR CONTROL FEATURE OFFERED BEFORE BEING ABLE TO ACTUALLY USE THE SERVICE	CHANNEL		STRATEGY		
		PLAY STORE	SERVICE PRESENTATION	INFORMATION ONLY	AUTHORIZATION HEADS-UP	EARLY CONTROL
Truecaller	In the Play Store page, you are informed that the app does not share information of your phonebook.	x			x	
	In the service presentation, you are informed that the app requires to access your call history, your contact list and SMS in order to work properly.		x		x	
	In the service presentation, you are informed that some data (name, phone number, IP address, etc.) are collected and analysed.		x	x		
	In the service presentation, you are informed that the collected data are used to improve, analyse and personalize the service that is offered.		x	x		
	In the service presentation, you are informed that the collected data are used to adhere to laws and protect users' security.		x	x		
	In the service presentation, you are informed that the collected data are used, after de-identification to generate reports and statistical analysis.		x	x		
	In the service presentation, you can allow the app to collect your data to personalize the ads you see.		x			x
		YES	YES	YES	YES	YES

Data regarding each single case are reported in Appendix B. A summary is presented below.

APP	CHANNEL		STRATEGY		
	PLAY STORE	SERVICE PRESENTATION	INFORMATION ONLY	AUTHORIZATION HEADS-UP	EARLY CONTROL
WHATSAPP	YES	YES	YES	YES	NO
FACEBOOK	NO	YES	NO	YES	NO
GOOGLE CHROME	NO	YES	NO	NO	YES
MESSENGER	NO	YES	NO	YES	NO
SUBWAY SURFERS	NO	YES	YES	NO	YES
TIKTOK	YES	YES	YES	NO	YES
CANDY CRUSH SAGA	YES	NO	YES	NO	NO
SHAREIT	YES	YES	YES	YES	NO
NETFLIX	YES	NO	YES	NO	NO
MICROSOFT WORD	YES	NO	YES	NO	NO
HANGOUTS	NO	YES	NO	YES	NO
MESSAGES	NO	YES	NO	NO	YES
SAMSUNG INTERNET BROWSER	YES	YES	NO	YES	YES
MICROSOFT EXCEL	YES	NO	YES	NO	NO
MICROSOFT POWERPOINT	YES	NO	YES	NO	NO
GOOGLE CALENDAR	YES	YES	YES	NO	NO
GOOGLE DOCS	YES	NO	NO	YES	NO
SAMSUNG HEALTH	NO	YES	NO	NO	YES
GOOGLE KEEP	YES	NO	NO	YES	NO
GARENA FREE FIRE	NO	YES	NO	YES	NO
MY TALKING TOM	NO	YES	NO	NO	YES
VIBER MESSENGER	NO	YES	YES	NO	YES
TRUECALLER	YES	YES	YES	YES	YES

APP	CHANNEL		STRATEGY		
	PLAY STORE	SERVICE PRESENTATION	INFORMATION ONLY	AUTHORIZATION HEADS-UP	EARLY CONTROL
MY TALKING ANGELA	NO	YES	NO	NO	YES
LINE	YES	YES	NO	YES	NO
TEMPLE RUN 2	NO	YES	YES	NO	YES
GOOGLE TRANSLATE	YES	YES	NO	YES	YES
OPERA MINI	YES	YES	YES	NO	YES
TELEGRAM	YES	YES	YES	NO	NO
B612	YES	YES	NO	YES	NO
IMO	NO	YES	NO	YES	NO
TEMPLE RUN	NO	YES	YES	NO	YES
FILES BY GOOGLE	NO	YES	NO	YES	NO
MICROSOFT SWIFTKEY KEYBOARD	YES	YES	YES	NO	YES
TOTAL YES	19	27	17	15	15
TOTAL YES (%)	26.8%	38.0%	50.0%	44.1%	44.1%

Table 13: Proactivity channels and strategies

Proactivity level and channels

The 34 apps following a proactive approach represent about half of the sample (47.9%). The most common channel to adopt such approach is the Service Presentation (38.0%). However, a relevant group use both: 16.9% (it represents more than a third of the proactive apps).

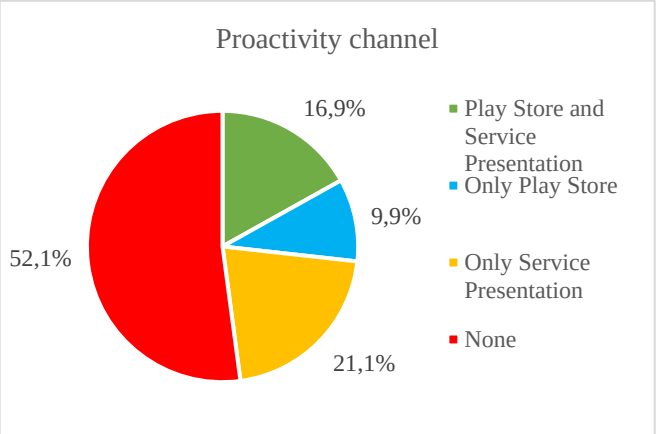

Figure 14: Distribution of proactivity channels

Proactivity strategies

The most adopted strategy is Information Only (50% of the proactive apps), meaning that proactive apps mainly try addressing privacy concerns at the first interaction with the users by offering some sort of transparency on data practices. However, it should be noted that the distribution of the strategies does not point out a clear preference, as all of them range in 6% interval.

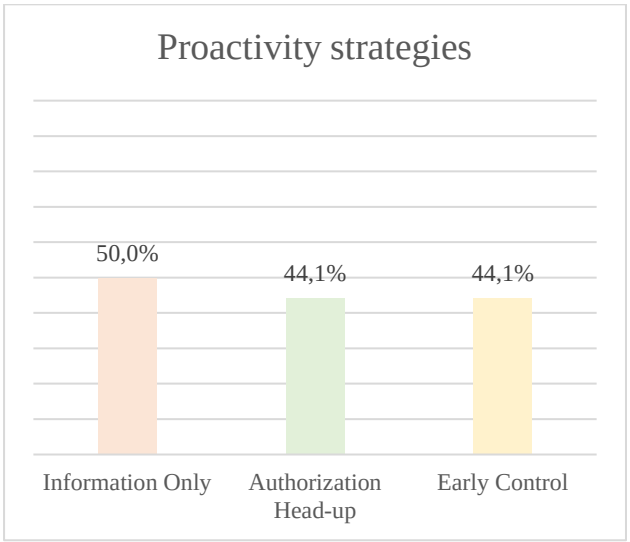

Figure 15: Distribution of proactivity strategies

Below, a more detailed explanation of each of the strategies is presented, together with representative examples.

Information only

Apps following this strategy use either the Play Store Page or the Service Activation to communicate some kind of information to the user about how his/her data will be treated, but without offering any options to control such treatment contextually.

For example, Microsoft Word, Excel and PowerPoint use their Play Store page to say that: *"Data provided through the use of this store and this app may be accessible to Microsoft or the third-party app publisher, as applicable, and transferred to, stored, and processed in the United States or any other country where Microsoft or the app publisher and their affiliates or service providers maintain facilities."*

TikTok highlights the personalization of its content and the data thanks to which it is possible: "*Watch endless amount of videos customized specifically for you: a personalized video feed based on what you watch, like, and share"*.

Candy Crush Saga try addressing users concerned about their data: "*Do not sell my data: King shares your personal information with advertising partners to personalize ads. Learn more at https://king.com/privacyPolicy. If you wish to exercise your Do Not Sell My Data rights, you can do so by contacting us via the in-game help centre or by going to https://soporto.king.com/contact*").

On the other hand, in the service presentation SHAREit gives a series of informative messages (the agreement is mandatory to use the app, hence it has not been considered a *control* feature) at the first launch of the app, briefly explaining that:

- The data that the app collects will be moved and treated in China.
- The app collects information to personalize the user's experience and the ads he sees.

Screenshots of the user experience are here reported, together with other interesting examples (Subway Surfers and Truecaller).

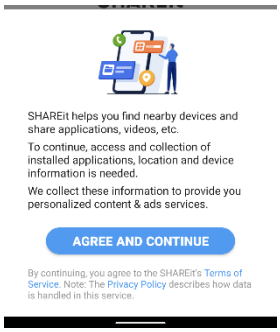

Figure 19: SHAREit communnications regarding data practices

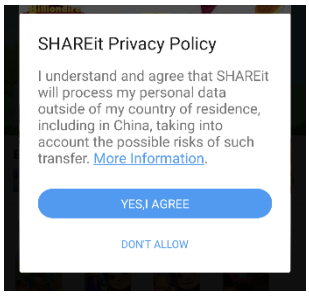

Figure 17: SHAREit warning about where the data will be processed

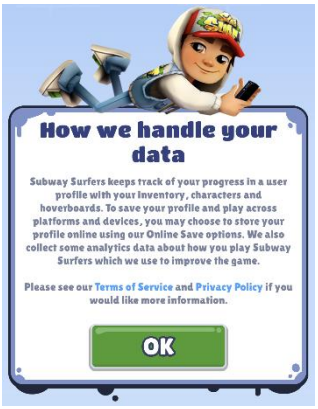

Figure 18: Subway Surfers' explanation about how data will be used

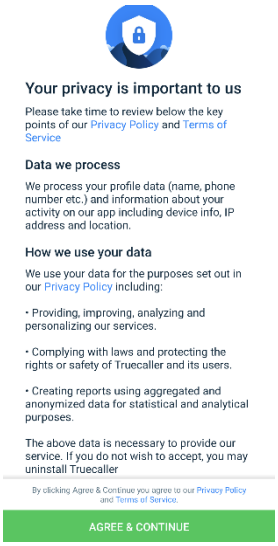

Figure 16: Truecaller communication regarding data practices

Authorization Heads-up

Apps following the *Authorization Head-up* strategy use either the Play Store Page or some dedicated pop-ups in the service presentation to explain why the user is asked by its own device to grant some specific permissions (e.g., camera, storage, phonebook, etc.).

For example, Samsung Internet Browser communicates required and optional permissions in the Play Store page:

"[Required permissions]:

- *None*

[Optional permissions]:

- *Location: Used to provide location-based content requested by the user or location information requested by the webpage in use*
- *Camera: Used to provide webpage shooting function and QR code shooting function*
- *Microphone: Used to provide recording function on webpage*
- *Contacts: Used to get the device account information for cloud sync*
- *Storage: Used to store files when downloading from webpages"*

The first time an app needs specific permissions to the device, the smartphone OS asks the user whether he wants to grant such request or forbid it with a standardized message, as explained in the Research Design chapter (pag. 45). Apps following the Authorization Heads-up strategy in the service presentation pre-alert the user with a customized pop-up that informs them that the device is going to ask whether to grant some permissions to the app, why and what happens if denies it. Here reported are some examples.

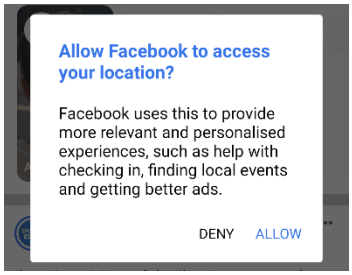

Figure 22: Facebook pop-up regarding access to the device's location

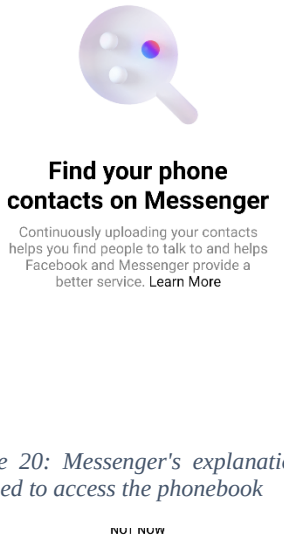

Figure 20: Messenger's explanation of the need to access the phonebook

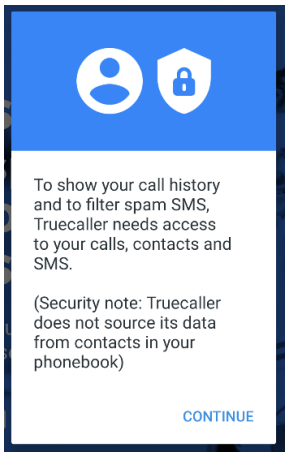

Figure 21: Truecaller's explanation about the access to the call history, phonebook and SMS

Early Control

Early Control can be provided only in the service presentation, as the Play Store page can be used only to download the app.

Subway Surfers offers a simple but valuable example of this strategy: before start playing, the user is asked whether he wants his/her advertising experience to be improved. In the same message, the app explains what it means: how the user experience will be affected, what data need to be collected and how they are going to be treated to be able to offer such experience. My Talking Tom adds an additional control: while deciding whether to allow the usage of data for improving the advertising experience, the user can even decide the specific partners with whom the app is allowed to share the data.

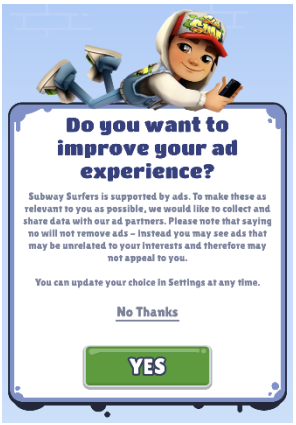

Figure 26: Subway Surfers' option to control the personalization of ads

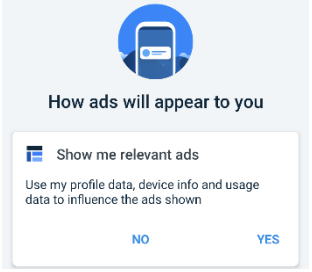

Figure 23: Truecaller's option to control the personalization of ads

Figure 25: My Talking Tom's menu to control the personalization of ads

Figure 24: My Talking Tom's menu to control the partner with whom data can be shared

Finally, Viber Messenger allows the management of a complex suite of privacy settings before the completion of the app initialization with an extensive number of controls. Despite such controls being very numerous and possibly overwhelming for the user's attention in the service presentation, they have a high level of detail and thorough descriptions.

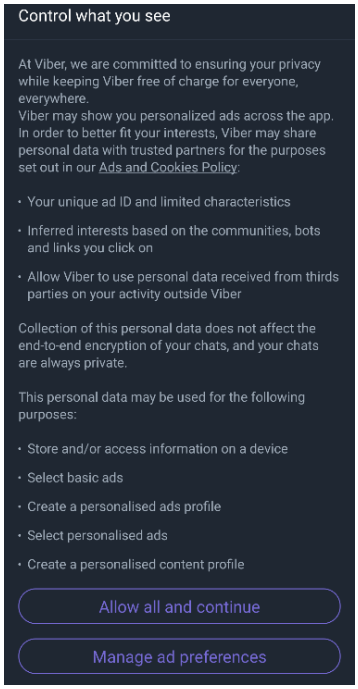

Figure 29: Viber's privacy settings (1)

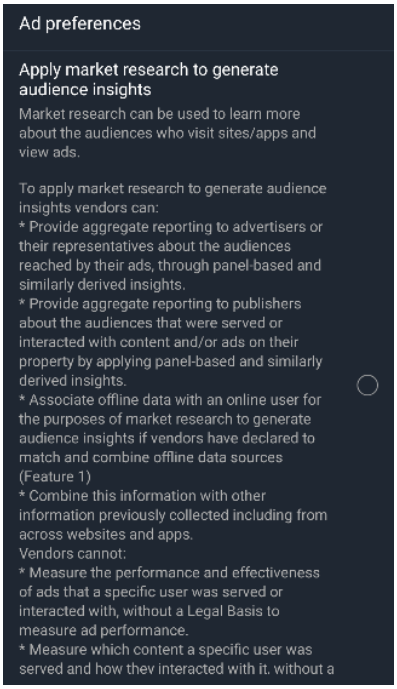

Figure 30: Viber's privacy settings (2)

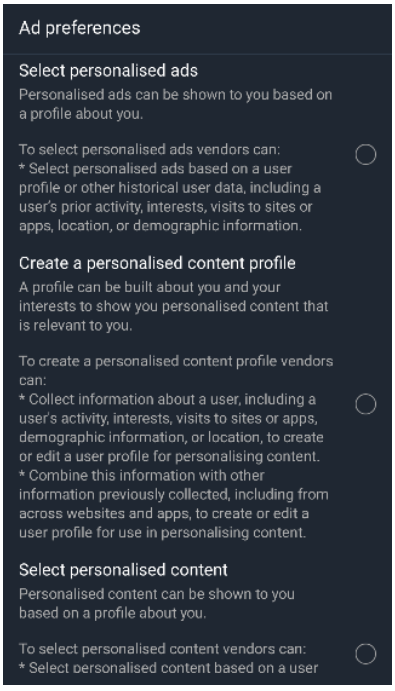

Figure 27: Viber's privacy settings (3)

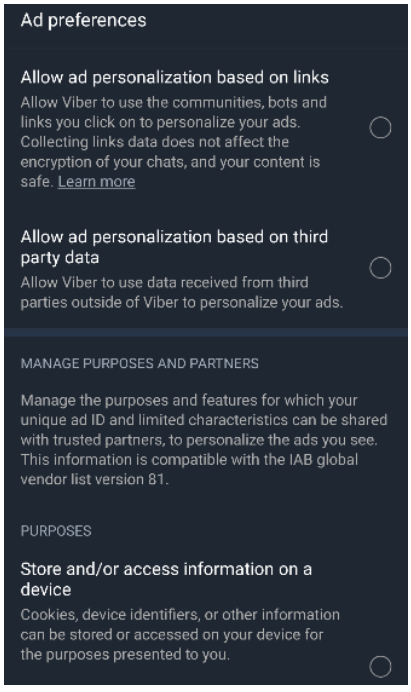

Figure 28: Viber's privacy settings (4)

5.3 Contributions

The results emerged from the two analysis allow to evaluate whether the strategies that the market is adopting are consistent with literature findings over the privacy research. First, the analysis of the descriptive metrics confirms that firms are actually implementing both Transparency and Control, whose effects on consumers behaviour are the subjects of numerous researches (e.g., Trabucchi, et al., 2019; Libaque-Sáenz, et al., 2020; Bornschein, et al., 2020). However, the sample presents a higher density below the averages for both Transparency and Control levels, meaning that the market is actually composed by many players offering low Transparency and Control and few ones strongly implementing both of them.

Transparency's adoption more than doubles the implementation of Control: if interpreted with the "Internet Users' Information Privacy Concerns" dimensions for privacy concerns (Malhotra, et al., 2004), it means that firms prefer to address the "awareness" concern (understanding about established conditions and actual practices) rather than the "control" one (the freedom to voice an opinion or exit). On the one hand, Transparency alone is a determinant of perceived control (Armitage, et al., 1999; Ajzen, et al., 1991; Wortman, 1975). On the other hand, informing users about data practices without offering some controls to exercise power over them could cause an increase in Perceived Information Risk without an adequate counterbalance on Perceived Data Control, resulting in raising privacy concerns and decreasing willingness to disclose information (Bornschein, et al., 2020).

The assessment model has been based on literature on Transparency's and Control's definitions and its design allows to evaluate how their implementation targets privacy concerns about Collection, Internal Unauthorized Use and External Unauthorized Use defined in the Concerns For Information Privacy (Smith, et al., 1996), and pursue the Access Fair Information Practice (Federal Trade Commission, 2020), which addresses also the "Error" concern among the Concerns For Information Privacy, through the 4 areas of measurement: Collection, Usage, Sharing, Access.

The "Collection" privacy concern (Smith, et al., 1996) is the most addressed one: apparently, the type of data involved and how they are collected are the most popular topic for the communication between users and providers. Also, the possibility to control whether data are collected and which data are collected are the options mostly granted to end-users. The concerns about the "Internal Unauthorized Use" privacy concern (Smith, et al., 1996) are preferably addressed with a transparent strategy rather than a control one, meaning that digital

services limit themselves to explain how data are used, rather than allowing the user to manage consent for specific purposes. Practices adopted to target such concern could be particularly interesting for apps leveraging data to support user research, such as the ones following a "e-ethnography" strategy (Trabucchi, et al., 2017a) . The "External Unauthorized Use" (Smith, et al., 1996) concern is treated differently: information about how data are shared with third parties are often coupled with the possibility to decide about such practices, and this could be an interesting indication for firms that share data to have an additional revenue stream, such as the ones following a "data trading" strategy (Trabucchi, et al., 2017a). Finally, the "Access" principle (Federal Trade Commission, 2020) is pursued with a balanced equilibrium between transparency (visibility over specific information collected) and control (possibility to update or delete specific information collected).

The industry analysis has shown that apps belonging to the "Social" category are leading the market towards increasing levels of transparency and control. Apps belonging to these categories generally have business models strongly dependent on data, such as the "enhanced advertising" strategy (Trabucchi, et al., 2017a) which leverages the analysis of personal information of the users to improve the effectiveness of the advertising messages. The effect of privacy concerns over willingness to disclose personal information (Min, et al., 2015) is a reasonable motive to encourage players of this industry to implement Transparency and Control in their value proposition.

Finally, the assessment model per se is a theoretical contribution to future research in privacy and digital services. It combines results of privacy, transparency, and control literature, and can be used as a powerful tool for market screening, to evaluate the implementation of transparency, control, and possible new levers usable to address privacy concerns. Also, the collected data can be used as a benchmark for successive research on alternative markets, niches of the app market, or to monitor how the behaviour of the sample will evolve in the long term.

As regards the proactive strategies, firms using the service presentation to adopt the "Information Only" strategy offer a realistic representation of the experiment scenario designed by Trabucchi and colleagues (2019) to evaluate the effects of Business Model Transparency. Based on their results, firms following this strategy can expect a higher willingness to use their services in individuals with high privacy concerns and in consumers that are used to more "opaque" business models. However, informing consumers about data practices could rise Perceived Information Risks, which could be counterbalanced by Perceived Data Control (Bornschein, et al., 2020): a practice that appears to be adopted by firms pursuing the "Early Control" strategy, which may represent the best way to address privacy concerns with a proactive approach.

6. Conclusions

The results of the research generate numerous insights regarding how the concept of privacy affects innovative business models that are based on data. The sample and the data collected about its units offer a representative view of how data driven business model are coping with the rising importance of privacy, which is determined by the increasing diffusion of business models that leverage Big Data to create value, such as two-sided platforms, and the recent scandals involving firms using such models.

Apparently, the mobile apps market is moving towards the implementation of Transparency and Control, leaded by a small portion that has more interest in addressing privacy concerns and mitigating their effects on behavioural intention. For now, Transparency is the most adopted lever, and this presents a possible criticality and area of improvement: notice should be balanced by power as much as possible to avoid the perception of risk to furtherly increase privacy concerns.

At the moment, firms are focusing their efforts on decreasing user's concerns about what types of data are collected and how they are collected by providing information about it and options to control such practices. Concerns about how data are used are addressed more with information rather than with options, if compared to how the other concerns are handled: the possibility to control data usage is satisfied mainly with power over data collection, without granting granular controls over how data are used after that the user has agreed to their collection. On the other hand, concerns about data sharing practices and the possibility to access the specific information that have been collected are addressed with a quite balanced approach of transparency and control. Sharing data is a hot practice now, frequently discussed by public opinion and apparently digital services providers are coping with the raise of concerns regarding these activities by granting a higher level of control (compared to other concerns) over the practices that are communicated to the user.

Apps belonging to the "Social" and "Communication" category are the ones with the highest levels of Transparency and Control: the importance of data in their business model is probably boosting the interest they have in mitigating the effects of privacy concerns over behavioural intention. In fact, social media and messaging app typically are entrusted with personal and sensitive information of the individual (e.g., private conversations, personal pictures, passions, opinions …) and their power over such information and relevance in people's life is often subject of debate and can be a cause for increasing privacy concerns.

The systematic analysis of 71 apps among the most downloaded ones enabled the possibility to observe a recurring strategy used to address privacy concern: almost half of the sample offers some kind of information and control to users before actually start using the app and its features, following a proactive approach to address privacy concerns.

In particular, two channels and three strategies are adopted to follow such approach: proactive apps use both the Play Store page (27% of the whole sample) and few screens with messages and options in the service initialization (38% of the whole sample) to present their data practices and offer some options to control them.

Proactive apps are currently following three non-exclusive strategies offering: (1) some kind of information about data practices without any control about them, (2) information and controls dedicated to the access to the smartphone sensors and data before requesting it to the system, and (3) few options to personalize how personal data will be treated by the app.

A proactive strategy addresses privacy concerns in the early stages of the interaction with a potential customer and may be a more effective way to provide knowledge and power to users, if compared to offering numerous messages and options in the settings. On the other hand, transparency and control must not be limited at first contact: one of the rights enforced by the GDPR is the possibility to withdraw the consent to data treatment at any time (Art. 7.3 “The data subject shall have the right to withdraw his or her consent at any time, General Data Protection Regulation (2016)).

In conclusion, firms leveraging data driven business models are currently including Transparency and Control in their value proposition, as two levers to mitigate the effects of privacy concerns on behavioural intention. The new regulatory frameworks and the raising interest of public opinion on data are influencing the market of digital services, and new practices addressing privacy are emerging. Giving users knowledge and power over their data is already being used as an attribute to differentiate from the market, in addition to complying with law.

Bibliography

ANDROIDRANK. [Online] [Cited: 20 February 2021.] androidrank.org.

Ajzen, Icek and Driver, B. L. 1991. Prediction of Leisure Participation from Behavioral, Normative, and Control Beliefs: An Application of the Theory of Planned Behavior. *Leisure Sciences.* 1991, Vol. 13, 3.

Ajzen, Icek and Fishbein, Martin. 1975. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* s.l. : Addison-Wesley, 1975.

Ajzen, Icek. 2001. Nature and Operation of Attitudes. *Annual Review of Psychology.* 2001, Vol. 52.

Amit, R. and Zott, C. 2001. Value creation in e-business. *Strategic Management Journal.* 2001, Vol. 22.

Armitage, C. J. and Conner, M. 1999. The Theory of Planned Behavior: Assessment of Predictive Validity and "Perceived Control". *British Journal of Social Psychology.* 1999, Vol. 38, 1.

Ataei, Mehrmaz, Degbelo, Auriol and Kray, Christian. 2018b. Privacy theory in practice: designing a user interface for managing location privacy on mobile devices. *Journal of Location Based Services.* 2018b, Vol. 12.

Ataei, Mehrnaz, et al. 2018a. Complying with Privacy Legislation: From Legal Text to Implementation of Privacy-Aware Location-Based Services. *International Journal of Geo-Information.* 2018a.

Atzori, L., Iera, A. and Morabito, G. 2010. The Internet of Things: a survey. *Computer Networks.* 2010, Vol. 54, 15.

Awad, Naveen Farag and Krishnan, M. S. 2006. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly.* 2006, Vol. 30, 1.

Bandyopadhyay, Soumava. 2009. Antecedents and consequences of consumers' online privacy concerns. *Journal of Business & Economics Research.* 2009.

Baruh, Lemi, Secinti, Ekin and Cemalcilar, Zeynep. 2017. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication.* 2017, Vol. 67, 1.

Bélanger, France and Crossler, Robert E. . 2011. Privacy in the Digital Age: A Review of Information Privacy Research in Information systems. *MIS Quarterly.* 2011, Vol. 35, 4.

Berger, C. 1993. Kano's methods for understanding customer-defined quality. *Center for quality management journal.* 1993, Vol. 2, 4.

Big Data: issues and challenges moving forward. **Kaisler, S., et al. 2013.** 2013.

Bornschein, Rico, Schmidt, Lennard and Maier, Erik. 2020. The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices. *Journal of Public Policy & Marketing.* 2020, Vol. 39, 2.

Brandimarte, L., Acquisti, Alessandro and Loewenstein, G. 2012. Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science.* 2012, Vol. 4, 3.

Buganza, Tommaso, et al. 2015. Unveiling the Potentialities Provided by New Technologies: A Process in Pursue Technology Epiphanies in the Smartphone App Industry. *Creativity and Innovation Management.* 2015, Vol. 24, 3.

Buganza, Tommaso, Trabucchi, Daniel and Pellizzoni, Elena. 2019. Limitless personalisation: the role of Big Data in unveiling service opportunities. *Technology Analysis & Strategic Management.* 2019.

Cadwalladr, Carole and Graham-Harrison, Emma. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian.* [Online] 17 March 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Candy Crush Saga. *Google Play Store.* [Online] https://play.google.com/store/apps/details?id=com.king.candycrushsaga&hl=en_US&gl=US.

Chang Liua, Jack T. Marchewkab, June Luc, Chun-Sheng Yud. 2005. Beyond concern - a privacy-trust-behavioral intention model of electronic commerce. *Information & Management.* 2005, 42.

Chang, Younghoon, et al. 2018. The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly.* 2018, Vol. 35.

Clarke, Roger. 1999. Internet Privacy Concerns confirm the case for Intervention. *Communications of the ACM.* 42, 1999, Vol. 2.

Cooley, Thomas M. 1880. *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract.* Chicago : Callaghan and Company, 1880.

Culnan, Mary J. and Armstrong, Pamela K. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science.* 1999, Vol. 10, 1.

Culnan, Mary J. and Bies, Robert J. 2003. Consumer privacy: balancing economic and justice consideration. *Journal of Social Issues.* 2003, Vol. 59, 2.

Das, T. K. and Teng, B. S. 2001. Trust, Control, and Risk in Strategic Alliances: An Integrated Framework. *Organization Studies.* 2001, Vol. 22, 2.

Del Vecchio, P., et al. 2018. Big Data for open innovation in SMEs and large corporations: trends, opportunities, and challenges. *Creativity and Innovation Management.* 2018, Vol. 27, 1.

Deloitte. 2017. *Global mobile consumer survey 2017.* 2017.

Diebold, F. X. 2012. A Personal Perspective on the Origin(s) and Development of "Big Data": The Phenomenon, the Term, and the Discipline. *Scholarly Paper ID 2202843.* 2012.

Dinev, Tamara and Hart, Paul. 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research.* 2006, Vol. 17, 1.

—. 2004. Internet privacy concerns and their antecedents - Measurement validity and a regression model. *Behavior and Information Technology.* 2004, Vol. 23, 6.

Dinev, Tamara, et al. 2013. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems.* 2013, Vol. 22, 3.

Downes, Larry and Numes, Paul. 2014. *Big Bang Disruption: Strategy in the Age of Devastating Innovation.* s.l. : Penguin, 2014.

Dunbar, Robin I. M. 2004. Gossip in Evolutionary Perspective. *Review of General Psychology.* 2004, Vol. 8, 2.

Dunfee, Thomas W., Smith, N. Craig and Ross Jr, William T. 1999. Social Contracts and Marketing Ethics. *Journal of Marketing.* 1999, Vol. 63.

Erevelles, S., Fukawa, N. and Swayne, L. 2016. Big data consumer analytics and the transformation of marketing. *Journal of Business Research.* 2016, Vol. 69.

European Union. 2016. General Data Protection Regulation. 2016.

Evans, D. S. 2003. The antitrust economics of multi-sided platform markets. *Yale Journal on Regulation.* 2003, Vol. 20.

Fan, W. and Bifet, A. 2013. Mining Big Data: current status, and forecast to the future. *ACM SIGKDD Explorations Newsletter.* 2013, Vol. 14, 2.

Federal Trade Commission. 2020. Privacy Online: Fair Information Practices in the electronic marketplace. 2020.

Filistrucchi, L., et al. 2014. Market definition in two!sided markets: Theory and practice. *Journal of Competition Law and Economics.* 2014, Vol. 10.

Foster, Eric K. 2004. Research on Gossip: Taxonomy, Methods, and Future Directions. *Review of General Psychology.* 2004, Vol. 8, 2.

Fox, Alexa K. and Royne, Marla B. 2018. Private information in a social world: assessing consumers' fear and understanding of social media privacy. *Journal of Marketing Theory and Practice.* 2018, Vol. 26.

Foxman, Ellen R. and Kilcoyne, Paula. 1993. Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues. *Journal of Public Policy & Marketing.* 1993, Vol. 12, 1.

Galunic, D. C. and Eisenhardt, K. M. 2001. Architectural innovation and modular corporate forms. *Academy og Management Journal.* 2001, Vol. 44.

Gandomi, Amir and Haider, Murtaza. 2015. Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management.* 2015, Vol. 35.

Gartner. Gartner IT Glossary. [Online] https://www.gartner.com/en/information-technology/glossary/big-data.

Google Play Store. [Online] https://play.google.com/store/apps.

Grzegorz Mazurek, Karolina Małagocka. 2019. What if you ask and they say yes? Consumers' willingness to disclose personal data is stronger than you think. *Business Horizons.* 2019, Vol. 62.

Hamid R. Nemati, Thomas Van Dyke. 2009. Do Privacy Statements Really Work? The Effect of Privacy Statements and Fair Information Practices on Trust and Perceived Risk in E-

Commerce. *International Journal of Information Security and Privacy, Volume 3, Issue 1.* 2009.

Harris, Peter. 1995. Sufficient Grounds for Optimism?: The Relationship Between Perceived Controllability and Optimistic Bias. *Journal of Social and Clinical Psychology.* 1995, Vol. 15, 1.

Hartmann, P. M., et al. 2016. Capturing value from big data - a taxonomy of data-driven business models used by start-up firms. *International Journal of Operations & Production Management.* 2016, Vol. 36, 10.

Hashem, Ibrahim Abaker Targio, Yaqoob, Ibrar and Anuar, Nor Badrul. 2015. The rise of "big data" on cloud computing: Review and open research issues. *Information Systems.* 2015, Vol. 47.

Hunter, Gary L. and Taylor, Steven A. 2020. The relationship between preference for privacy and social media usage. *Journal of Consumer Marketing.* 2020, Vol. 37, 1.

Kaiser, Brittany. 2019. *Targeted:My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy.* s.l. : HarperCollins Publishers, 2019.

Klein, Cynthia T.F. and Helweg-Larsen, Marie. 2002. Perceived control and the optimistic bias: A meta-analytic review. *Psychology and Health.* 2002, Vol. 17, 4.

Kokolakis, Spyros. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security.* 2017.

Li, Ting and Unger, Till. 2012. Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems.* 2012, Vol. 21, 6.

Li, Yuan. 2001. Empirical studies on online information privacy concerns: literature review. *Communications of the Association for Information Systems.* 2001, Vol. 28, 1.

—. 2012. Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems.* 2012, Vol. 54.

Libaque-Sáenz, Christian Fernando, et al. 2020. The effect of Fair information practices and data collection methods on privacy-related behaviors: A study of Mobile apps. *Information & Management.* 2020.

Libaque-Sáenz, Christian Fernando, et al. 2016. Understanding antecedents to perceived information risks: An empirical study of the Korean telecommunications market. *Information Development.* 2016, Vol. 32, 1.

Lohr, R. 2012. The age of Big Data. *The New York Times.* 11 February 2012.

Malhotra, Naresh K. , Kim, Sung S. and Agarwal, James. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research.* 2004, Vol. 15, 4.

Manyika, J., et al. 2011. Big data: The next frontier for innovation, competition, and productivity. 2011.

Margulis, Stephen T. 2003. On the status and contribution of Westin's and. *J. Soc. Issues.* 2003, Vol. 59, 2.

—. 2003. Privacy as a Social Issue and Behavioral Concept. *J. Soc. Issues.* 2003, Vol. 59, 2.

Marston, S., et al. 2011. Cloud computing - the business perspective. *Decision Support Systems.* 2011, Vol. 51, 1.

Martin, Kelly D. and Murphy, Patrick E. 2016. The role of data privacy in marketing. *Journal of the Academy of Marketing Science.* 2016, Vol. 45, 2.

Martin, Kelly D., Borah, Abhishek and Palma, Robert W. 2017. Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing,.* 2017, Vol. 81.

McAfee, A. and Brynjolfsson, E. 2012. Big Data: the management revolution. *Harvard Business Review.* 2012, Vol. 90, 10.

McDonald, A. and Cranor, L. F,. 2008. The cost of reading privacy policies. *I/S: a journal of law and policy for the information society.* 2008.

Microsoft World. *Google Play Store.* [Online] https://play.google.com/store/apps/details?id=com.microsoft.office.word&hl=en_US&gl=US .

Milne, G. R,. and Rohm, A. 2000. Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *J. Public Policy and Marketing* . 2000, Vol. 19, 2.

Milne, G. R. and Boza, M. E. 1999. Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing.* 1999, Vol. 13, 1.

Milne, George R. and Culnan, Mary J. 2004. Strategies for reducing online privacy risks. Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing.* 2004, Vol. 18, 3.

Min, Jinyoung and Kim, Byoungsoo. 2015. How Are People Enticed to Disclose Personal Information Despite Privacy Concerns in Social Network Sites? The Calculus Between Benefit and Cost. *Journal of the Association for Information Science and Technology.* 2015, Vol. 66, 4.

Nemati, Hamid R. and Van Dyke, Thomas. 2009. Do Privacy Statements Really Work? The Effect of Privacy Statements and Fair Information Practices on Trust and Perceived Risk in E-Commerce. *International Journal of Information Security and Privacy.* 2009, Vol. 3, 1.

Norberg, Patricia A., Horne, Daniel R. and Horne, David A. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of consumer Affairs.* 2007, Vol. 41, 1.

Organization for Economic Cooperation and Development. 1980. Guidelines on the protection of privacy and transborder flows of personal data. Washington DC : s.n., 1980.

Parker, Geoffrey G., Van Alstyne, Marshall W. and Choudary, Sangeet Paul. 2017. *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You.* s.l. : W. W. Norton & Co. Inc., 2017.

Phelps, J., Nowak, G. and Ferrell, E. 2000. Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *J. Public Policy and Marketing* . 2000, Vol. 19, 2.

Privacy in Electronic Commerce and the Economics of Immediate Gratification. **Acquisti, Alessandro. 2004.** New York : Association for Computing Machinery, 2004. EC '04: Proceedings of the 5th ACM conference on Electronic commerce.

Raschke, Philip, et al. 2018. Designing a GDPR-compliant and Usable Privacy Dashboard. *Privacy and Identity Management. The Smart Revolution.* 2018.

Rosenberg, Matthew, Confessore, Nicholas and Cadwalladr, Carole. 2018. How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times.* [Online] 17 March 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?.

Rossi, Arianna and Lenzini, Gabriele. 2020. Transparency by design in data-informed research: A collection of information design patterns. *Computer law & security review.* 2020, Vol. 37.

Samsung Internet Browser. *Google Play Store.* [Online] https://play.google.com/store/apps/details?id=com.sec.android.app.sbrowser&hl=en_US&gl=US.

Schwaig, Kathy Stewart, Kane, Gerald C. and Storey, Veda C. 2006. Compliance to the fair information practices: How are theFortune 500 handling online privacy disclosures? *Information & Management.* 2006, Vol. 43.

Sheehan, Kim Bartel and Hoy, Mariea Grubbs. 2000. Dimensions of privacy concerns among online consumers. *Journal of Public Policy & Marketing.* 2000, Vol. 19, 1.

—. 1999. Flaming, Complaining, Abstaining. How Online users respond to privacy concerns. *Journal of Advertising.* 1999, Vol. 28, 3.

Skinner, E. A. 1996. A guide to constructs of control. *Journal of Personality and Social Psychology.* 1996, Vol. 71, 3.

Smith, H. Jeff, Dinev, Tamara and Xu, Heng. 2011. Information privacy research, an interdisciplinary review. *MIS Quarterly.* 2011, Vol. 35, 4.

Smith, H. Jeff, Milberg, Sandra J. and Burke, Sandra J. 1996. Information Privacy: Measuring Individuals Concerns About Organizational Practices. *MIS Quarterly.* 1996, Vol. 20, 2.

Solove, Daniel J. 2002. Conceptualizing Privacy. *California Law Review.* 2002, Vol. 90, 4.

Solove, Daniel J. 2008. *Understanding Privacy.* s.l. : Harvard University Press, 2008.

Stewart, Kathy A. and Segars, Albert H. 2002. An empirical examination of the concern for information privacy instrument. 2002, Vol. 13, 1.

Stone, et al. 1983. A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology.* 1983, Vol. Vol 68, 3.

The effects of self-construal and perceived control on privacy concerns. **Xu, Heng. 2007.** Montréal : s.n., 2007. Proceedings of the 28th Annual International Conference on Information Systems.

Tik Tok. *Google Play Store.* [Online] https://play.google.com/store/apps/details?id=com.zhiliaoapp.musically&hl=en_US&gl=US.

Trabucchi, Daniel and Buganza, Tommaso. 2018. Data-driven innovation: switching the perspective on Big Data. *European Journal of Innovation Management.* 2018.

—. 2019. Fostering digital platform innovation: From two to multi-sided platforms. *Creativity and Innovation Management.* 2019.

Trabucchi, Daniel, Buganza, Tommaso and Patrucco, A. 2019. Business Model Transparency: do you care how digital platforms use your data? 2019.

Trabucchi, Daniel, Buganza, Tommaso and Pellizzoni, Elena. 2017a. Give away your digital services, leveraging Big Data to capture value. *Research-Technology Management.* 2017a.

Trabucchi, Daniel, et al. 2017b. Exploring the inbound and outbound strategies enabled by user generated big data: Evidence from leading smartphone applications. *Creativity Innovation Management.* 2017b.

Tucker, C. E. 2014. Social networks, personalized advertising and privacy controls. *Journal of Marketing Research.* 2014, Vol. 51.

U. S. Supreme Court. 1928. Olmstead v. United States, 277 U.S. 438. 1928.

Vajjhala, N. R. and Ramollari, E. 2016. Big Data using cloud computing-opportunities for small and medium-sized enterprises. *European Journal of Economics and Business Studies.* 2016, Vol. 4, 1.

Waldo, J., Lin, H. and Millet, L. I. 2007. *Engaging Privacy and Information Technology in a Digital Age.* Washington DC : National Academies Press, 2007.

Wamba-Fosso, S., et al. 2015. How 'Big Data' can make big impact: findings from a systematic review and a longitudinal case study. *International Journal of Production Economics.* 2015, Vol. 165.

Warren, Samuel D. and Brandeis, Louis D. 1890. The right to privacy. *Harvard Law Review , Vol. 4, No. 5.* 15 Dec 1890, pp. 193-220.

Westin, A. F. 1967. *Privacy and Freedom.* New York : Atheneum, 1967.

Wortman, C. 1975. Some Determinants of Perceived Control. *Journal of Personality and Social Psychology.* 1975, Vol. 31, 2.

Wua, Kuang-Wen, Huang, Shaio Yan and Yen, David C. 2012. The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior.* 2012, Vol. 28.

Wylie, Christopher. 2019. *Mindf*ck - Inside Cambridge Analytica's Plot to Break the World.* s.l. : Profile Books Ltd, 2019.

Xu, Heng, et al. 2012. Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Service. *Information Systems.* 2012, Vol. 23, 4.

Xu, Heng, et al. 2011. Information Privacy Concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems.* 2011, Vol. 12, 12.

Yin, R. K. 2013. *Case study research: Design and methods.* s.l. : Thousand Oaks, CA: Sage Publications, 2013.

Zhang, Wang and Hsu. 2019. The effects of voluntary GDPR adoption and the readability of privacy statements on customers' information disclosure intention and trust. *Journal of Intellectual Capital.* 2019.

Appendix A: Sample details

APP	TRANSPARENCY/CONTROL FEATURES ADDRESSING SPECIFIC DATA TREATMENT OVER SPECIFIC DATA TYPES	TRANSPARENCY				CONTROL			
		COLLECTION	USAGE	SHARING	ACCESS	COLLECTION	USAGE	SHARING	ACCESS
Whatsapp	You are informed that the app needs to read the data in your phonebook to connect you to your contacts in the app's network.	x	x						
	You are informed that you can allow the app to access your contacts, pictures and storage to restore your personal Cloud backup.	x	x						
	You can download all your data. There are some examples of the types of data collected and it is clarified that the content of the chats is not accessible because it is not collected.	x			x				
	You can delete your data by deleting the account.								x
		3	2	0	1	0	0	0	1
Facebook	You are informed that the app deduces your main location and uses it to personalize your experience. You can see the inferred location.	x	x		x				
	You can allow the app to collect your exact location to personalize your experience.	x	x			x			
	You can allow the app to collect the history of your whereabouts to personalize your experience. You can see the history and delete it partially or completely.	x	x		x	x			x
	You can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network. You can stop the synchronization and delete the data that have been collected.	x	x			x			x
	You can see the types of data Facebook collects and download all of them.	x			x				
	You are informed that the app collects your search history. You can see it and delete it partially or completely.	x			x				x
	You are informed that the app collects your activities history. You can see it with the activities grouped by category.	x			x				
	You are informed that the app infers the topics you are interested in to personalize the ads you see. You can check and delete them.	x	x		x				x
	You can exert the GDPR right to object the usage of your data through a dedicated form.						x		
	You can allow the app to analyse your photos to try to recognize yourself in photos uploaded on the platform.	x	x				x		
	You are informed that the advertisers can use information on your profile to reach you/exclude you from their targeted segments. You can see who is using them for such purpose and decide what information can be used.	x		x	x	x			
	You can allow third-party apps and websites using Facebook for Business to share the information they collect about you with Facebook, which uses them to personalize the ads you see. You can see their identity, the number of interactions they have shared and download what they have shared. You can delete the information Facebook has received until now (but not stop the collection from	x		x	x			x	x

	Facebook settings, since the collections does not happen on Facebook).								
	You can allow advertisers to reach you outside the app by using Facebook for Business.			x				x	
	You can see the third-party apps or websites to which you have signed up using your Facebook account. You can see the type of data they can access, stop them from continuing and delete the information they have collected until now.	x		x				x	x
		12	6	4	8	4	2	3	6
YouTube	You can allow YouTube to collect your search history and use it to personalize your experience. You can see it, together with the details of the specific search, and delete it completely or partially.	x	x		x	x			x
	You are informed that you can allow YouTube to collect the history of what you watch and use it to personalize your experience. You can see it, together with the details of the specific activity, and delete it completely or partially.	x	x		x	x			x
	You can see the type of data YouTube collects and download all of them.	x			x				
	You can set the periodic elimination of the history of your activities on YouTube.								x
	You can see the list of third-party apps connected to your account. You can revoke the connection.			x				x	
	You are informed that other YouTube Apps share data about you with YouTube to personalize your experience.			x					
		3	2	2	3	2	0	1	3
Google Photos	You are informed that your activities with Google Lens inside Google Photos are saved in your Google Account if the collection of data on Google websites and apps is allowed.	x		x					
	You are informed that Google Photos uses the information of your whereabouts to personalize your experience.	x	x						
	You can allow Google Photos to analyse the faces in your photos to group them according to the subjects.	x	x				x		
		3	2	1	0	0	1	0	0
Google Chrome	You can allow the app to synchronize the information (password, browsing history, etc.) of your Google Account in order to personalize your experience, the ads you see and other Google Services.	x		x		x		x	
	You can allow the app to collect diagnostic data to improve the product.	x	x			x			
	You are informed that you can enable the “do not track” mode, but it is only a request to websites, who can decide to keep on using your cookies to personalize the ads you see.	x		x		x		x	
	You are informed about what cookies are and how they are used by the websites you visit to track your browsing activities.	x		x					
	You can see the list of websites that have accessed your data. For every website, you can see the size of collected data.	x		x					
	You can disable the collection of cookies. You can delete the ones collected until now.					x		x	x
	You can disable the collection of third-party cookies.					x		x	

	You can specify a website for which you want to allow the collection of cookies.							x	
	For every website, you can see the authorizations you granted.	x		x					
	You can decide whether websites must ask for your permission before accessing your location.					x		x	
	You can decide whether websites must ask for your permission before accessing your camera.					x		x	
	You can decide whether websites must ask for your permission before accessing your microphone.					x		x	
	You can decide whether websites can access to your motion sensors.					x		x	
	You can see your browsing history and delete it partially or completely.	x			x	x			x
		7	1	5	1	10	0	9	2
Google (general)	You can allow Google to collect the data of your activities on Google websites and apps to personalize your experience using Google Services. You can see the history of the activities, access the details of their collection and delete it completely or partially.	x	x		x	x			x
	You can allow Google to collect the history of your whereabouts, even when you are not using Google services, to personalize your experience using Google Services. You can see the history, access the details of the collection of each location and delete it completely or partially.	x	x		x	x			x
	You can allow Google to collect the data of your activities on the apps in your device (note: that refers to all the apps, not only the Google ones) to personalize your experience using Google Services. You can see the history of the activities, access the details of their collection, and delete it completely or partially.	x	x		x	x			x
	You can allow Google to collect the recordings of the conversations with Google Assistant to personalize your experience using Google Services	x	x			x			
	You can see all the types of data that Google collects about you and download them. You can delete your account and all the data it contains.	x			x				x
	You can set the periodic elimination of the history of your activities on websites and apps using Google Services.					x			
	You can set the periodic elimination of the history of your whereabouts.					x			
	You are informed that Google uses your personal information to personalize the ads you see on its apps and websites. That can happen also on external websites through AdSense. You can see, review and remove the topics of your interest that Google has inferred about you, revie to personalize the ads you see.	x	x	x	x		x	x	x
		6	5	1	5	6	1	1	5
Google Maps	You can see all the types of data that the app collects and download them.	x			x				
	You are informed that you can allow Google to collect the history of your whereabouts, even when you are not using Google services, to personalize your experience using Google Services. You can see the history, access the details of the collection of each location and delete it completely or partially.	x	x		x	x			x

	You can set the periodic elimination of the history of your whereabouts.					x			
	You are informed that you can allow Google Maps to receive information about your trip tickets shared from Gmail and Calendar to show you information about those trips on Maps.	x		x				x	
	You can allow Google Maps to collect information about your contacts to show you their location on Maps.	x	x				x		
		4	2	1	2	2	1	1	1
Instagram	You can see the list of your activities on Instagram that have been collected grouped by category.	x			x				
	Your searches with the search bar are collected. You can delete the search history partially or completely.	x			x				x
	You can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You are informed that the app uses your data to personalize the advertisement experience.		x						
	You can allow the app to use information shared by third parties to personalize the ads you see.			x				x	
	You are informed that Instagram does not share data with external advertisers.			x					
	You can see the list of your topics of interest that Instagram has inferred.	x			x				
	You can download all your data grouped by type.	x			x				
	You can see the list of the ads with which you have interacted.	x			x				
	You can see the list of third-party apps and websites where you have signed in with your Instagram account.			x					
		6	2	3	5	1	0	1	1
Messenger	You can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You can allow the app to send and receive SMS through the app.	x	x			x			
		2	2	0	0	2	0	0	0
Subway Surfers	You are informed that Subway Surfers collects the data of your activities in the app.	x							
	You are informed that Subway Surfers collects additional data to improve the app.		x						
	You are informed that you can allow Subway Surfers to collect and share your advertising ID with third-party advertisers to personalise the ads you see.	x		x		x			
		2	1	1	0	1	0	0	0
Tiktok	You can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You are informed that the videos you see are personalized according to what you watch, like and share	x	x						
	You can allow TikTok to use the data of your activities in the app to personalize the ads you see.	x	x				x		
	You can allow TikTok to collect data shared by its partners to personalize the ads you see.			x				x	

	You can see the identity of the partners that share data with TikTok			x					
	You can see the interests that TikTok has inferred about you.	x			x				
	You can download your data and delete it by deleting the account	x			x				x
	You can choose among a set of topics of interest through which TikTok can personalize your experience.	x	x			x			x
		6	4	2	2	2	1	1	2
Candy Crush Saga	You are informed that the app shares personal data with advertisers to personalize the ads you see			x					
	You are informed that you can forbid the app to share your personal data with advertisers by contacting the developer at the dedicated email address.			x					
		0	0	2	0	0	0	0	0
Snapchat	You can see the list of authorization you have granted.	x							
	You can see all the types of data Snapchat collects and download them.	x			x				
	You are informed that you can allow Snapchat to personalize the ads you see according to whether your profile fits particular segments.	x	x				x		
	You can see the third-party apps at which you have signed up using your Snapchat account and review the information they can collect.	x		x		x		x	
	You are informed that the connection with third party apps will be deleted after 90 day of non-usage.			x					
	You can allow Snapchat to share your data with third-party network advertisers to personalize its and their ads.			x				x	
	You are informed that you can allow Snapchat to receive and use the data of your activities outside the app to personalize the ads you see.			x				x	
	You can see your lifestyle and topics of interest that Snapchat has inferred about you to personalize the ads you see.	x	x		x				
	You are informed that your search history is collected. You can see it and review it	x			x				x
	The history of your whereabouts is collected	x			x	x			x
	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network. You can delete the data that have been collected.	x	x			x			x
		8	3	4	4	3	1	3	3
Twitter	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network. You can delete the data that have been collected.	x	x			x			x
	You can choose to allow the usage of your data to personalize the ads you see on Twitter.		x				x		
	You can choose to allow the usage of the data of your activities outside Twitter to personalize the ads you see on Twitter.	x		x				x	
	You are informed that you can allow the app to collect the data about your exact location to personalize your experience on Twitter.	x	x			x			

	You are informed that you can allow the app to collect the data about the places you visit to personalize your experience on Twitter.	x	x			x			
	You are informed that you can allow Twitter to use the topics of interest it inferred about you to personalize your experience on Twitter. You can see what has been inferred and remove the topics you are not interested in.	x	x		x		x		x
	You can see the list third-party apps connected to your account. You can disconnect it from them.			x				x	
	You are informed that you can allow the app to share your data with commercial partners.			x				x	
	You can download all your data.	x			x				
		6	5	3	2	3	2	3	2
SHAREit	You are informed that the app needs to access to the apps you have installed on your device, your location data and information about your device to work properly.	x	x						
	You are informed that the data that the app collects will be moved and treated in China.	x							
	You are informed that the app will not ask for permissions that are irrelevant to its functionality		x						
	You are informed that the app asks the permission to your Bluetooth settings to discover nearby users more quickly	x	x						
	You are informed that the app collects information to personalize your experience and the ads you see.		x						
	You are informed that you can allow the app to collect your location to help you discover nearby users.	x	x			x			
	You are informed that your search history is collected. You can see it and delete it partially or completely	x			x				x
	You are informed that you can allow the collection of the data of usage improve the app	x	x			x			
	You can delete your account and all the data contained.								x
		6	6	0	1	2	0	0	2
Google Play Games	You are informed that the data of Google Play Games are used to personalize your experience. You can delete them partially or completely	x	x						x
	You are informed that your search history is collected. You can see it and delete it partially or completely	x			x				x
	You can delete your Google Play Games Account and all the data it contains.								x
		2	1	0	1	0	0	0	3
Skype	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You are informed that you can allow the app to use the data of your location to improve your search results on Bing.	x		x				x	
	You are informed that you can allow some fragments of your conversations (after a de-identification process) to be analysed to improve Skype Translator.	x	x			x			

	You can delete your Microsoft account and all of the data contained in it.								x
		3	2	1	0	2	0	1	1
Netflix	You are informed that the more you use Netflix the better the suggestions will be.	x	x						
	You can download your data.	x			x				
	You are informed that you can allow the app to include you in experiments and previews to improve Netflix.		x				x		
		2	2	0	1	0	1	0	0
Google Duo	You are informed that your video/audio conversations are private thanks to end-to-end cryptography.	x							
	You are informed that the data of your face used to apply graphical filters are not stored in your Google Account.	x							
	You are informed that your message conversations are private thanks to end-to-end cryptography.	x							
	You can disconnect Duo from your Google Account					x			
	You are informed that you can allow the app to save videos, audio messages, photos and notes in Duo.	x				x			
	You can delete your Duo Account.								x
		4	0	0	0	2	0	0	1
Microsoft Word	You are informed that the data generated with the app usage may be accessible to Microsoft and third-party partners.	x		x					
	You are informed that the data generated with the app usage may be moved and treated in the United States.	x							
	You are informed that diagnostic data are collected to keep the app working properly. They are visible through a Diagnostic Data Viewer.	x	x		x				
	You are informed that you can allow the app to collect additional diagnostic data to improve the product.	x	x			x			
		4	2	1	1	1	0	0	0
Hangouts	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You are informed that you can allow the app to collect your phone number so that you can use the app to make calls and send SMS.	x	x			x			
	You are informed that you can allow the app to use diagnostic data to improve the app.	x	x				x		
		3	3	0	0	2	1	0	0
Messages	You are informed that you can allow the app to send information about your chats to Google to provide an anti-spam filter.	x		x				x	
	You are informed that answers and actions suggestions depend on the conversations but are generated on the device.	x	x	x					
	You are informed that you can allow the app to use some of the information in your conversations to show previews and spot dangerous content	x	x				x		
	You are informed that you can allow the app to read the phone number of commercial activities who texts you to verify their identity.	x	x				x		

		4	3	2	0	0	2	1	0
Samsung Internet Browser	You are informed about what optional permissions you can grant the app and why they are asked.	x	x						
	You are informed that your search history is collected. You can see it and delete it partially or completely.	x			x				x
	You are informed that your browsing history is collected. You can see it and delete it partially or completely.	x			x				x
	You are informed that you can allow the app to collect error logs to improve the product.	x	x			x			
	You are informed that you can enable/disable the synchronization with your Samsung Account to share your data across your devices and Samsung apps.	x		x		x		x	
	You can disable cookies.					x		x	
	You can disable third-party cookies					x		x	
	You can disable monitoring cookies					x		x	
	You can ask the websites you visit to not use cookies to track your activities					x		x	
		5	2	1	2	6	0	5	2
Microsoft Excel	You are informed that the data generated with the app usage may be accessible to Microsoft and third-party partners.	x		x					
	You are informed that the data generated with the app usage may be moved and treated in the United States.	x							
	You are informed that diagnostic data are collected to keep the app working properly. They are visible through a Diagnostic Data Viewer.	x	x		x				
	You are informed that you can allow the app to collect additional diagnostic data to improve the product.	x	x			x			
		4	2	1	1	1	0	0	0
Google Street View		0	0	0	0	0	0	0	0
One Drive	You are informed that diagnostic data are collected to keep the app working properly. They are visible through a Diagnostic Data Viewer.	x	x		x				
	You are informed that you can allow the app to collect additional diagnostic data to improve the product.	x	x			x			
		2	2	0	1	1	0	0	0
Dropbox	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You are informed that your search history is collected. You can see it and delete it partially or completely.	x			x				x
		2	1	0	1	1	0	0	1

Google Play Books		0	0	0	0	0	0	0	0
Microsoft PowerpPoint	You are informed that the data generated with the app usage may be accessible to Microsoft and third-party partners.	x		x					
	You are informed that the data generated with the app usage may be moved and treated in the United States.	x							
	You are informed that diagnostic data are collected to keep the app working properly. They are visible through a Diagnostic Data Viewer.	x	x		x				
	You are informed that you can allow the app to collect additional diagnostic data to improve the product.	x	x			x			
		4	2	1	1	1	0	0	0
Google Calendar	You are informed that the data about your position is used to personalize the graphic style of the Agenda.	x	x						
	You can allow the app to use your data from Gmail to show you events and bookings in the calendar	x		x				x	
		2	1	1	0	0	0	1	0
Google Docs	You are informed about what optional permissions you can grant the app and why they are asked.	x	x						
		1	1	0	0	0	0	0	0
Google News		0	0	0	0	0	0	0	0
Samsung Heath	You are informed that you can allow the app to collect health data.	x				x			
	You are informed that you can allow the app to use your data to personalize your experience		x				x		
	You are informed that you can allow the app to collect your position data	x				x			
	You can see the list of third-party apps you authorized to share data with the app. You can revoke the authorizations.			x				x	
	You are informed that you can enable/disable the synchronization with your Samsung Account to share your data across your devices and Samsung apps.	x		x		x		x	
	You can download your data	x			x				
		4	1	2	1	3	1	2	0

Google Keep	You are informed about what optional permissions you can grant the app and why they are asked.	x	x						
		1	1	0	0	0	0	0	0
Garena Free Fire	You are informed about what permissions you have to grant the app and why they are asked.	x	x						
		1	1	0	0	0	0	0	0
Clash of Clams	You are informed that you can allow the app to share your data to personalize the ads you see.	x		x				x	
		1	0	1	0	0	0	1	0
UC Broswer	You are informed that your search history is collected. You can see it and delete it partially or completely.	x			x				x
	You are informed that your browsing history is collected. You can see it and delete it partially or completely.	x			x				x
	You are informed that your navigation data are collected. You can delete them.	x							x
	You can enable the Incognito mode to avoid the collection of your browsing and search history.					x		x	
		3	0	0	2	1	0	1	3
Spotify		0	0	0	0	0	0	0	0
My Talking Tom	You are informed that you can allow the app and its partners to collect and analyse your data to personalize the ads you see.			x				x	
	You can see the specific partners with which the app share data, access their privacy policy and decide whether to allow their inclusion in the partners list.			x				x	
		0	0	2	0	0	0	2	0
Viber Messenger	You are informed that the content of your chats is not shared	x							
	You are informed that you can allow the app to personalize the ads you see according to the links you click.	x	x				x		
	You are informed that you can allow the app to personalize the ads you see according to information shared by external partners.			x				x	
	You are informed that you can allow external partners to save and read information on your device.	x		x				x	
	You are informed that you can allow external partners to infer your personal profile to personalize the ads you see.	x		x				x	
	You are informed that you can allow external partners to infer your personal profile to personalize the content you watch.	x		x				x	

	You are informed that you can allow external partners to monitor the effectiveness of the ads they show you.	x		x				x	
	You are informed that you can allow external partners to monitor the effectiveness of the content you watch.	x		x				x	
	You are informed that you can allow external partners to use the information they collect about you for market research.			x				x	
	You are informed that you can allow external partners to use the information they have about you for improving their products			x				x	
	You are informed that external partners aggregate different data sources to combine your information	x		x					
	You are informed that external partners aggregate data from different devices to combine your information	x		x					
	You are informed that the app share data with vendors to guarantee security, prevent frauds and debug			x					
	You are informed that you can allow external partners to read basic information that your device sends by default (e.g. IP Address) to identify it and show you personalized ads	x		x				x	
	You are informed that you can allow external partners to create digital IDs to identify and actively track your device	x		x		x			
	You can see the identity of the external partners and how they use the data shared by the app. You can decide whether to allow their inclusion in the partners list.			x				x	
	You are informed that you can allow external partners to use your exact location to personalize your experience.	x		x				x	
	You can download all your data	x			x				
	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You can eliminate your account and all the data it contains								x
		14	2	15	1	2	1	11	1
Truecaller	You are informed that the app does not share information of your contact list	x		x					
	You are informed that the app requires to access your call history, your contact list and SMS in order to work properly.	x	x						
	You are informed that some data of your profile are collected. You can seem them and request their deletion.	x			x				x
	You are informed that your data are collected to improve and personalize the service.		x						
	You are informed that your data are collected to adhere to laws and protect users' security		x						
	You are informed that your data are collected to generate reports and statistical analysis.		x						
	You are informed that you can allow the app to collect your data to personalize the ads you see.		x				x		
		3	5	1	1	0	1	0	1

My Talking Angela	You are informed that you can allow the app and its partners to collect and analyse your data to personalize the ads you see.			x				x	
	You can see the specific partners with which the app share data, access their privacy policy and decide whether to allow their inclusion in the partners list.			x				x	
		0	0	2	0	0	0	2	0
LINE	You are informed that you can allow the app to access your phone to collect your phone number and use it to create you an account.	x	x			x			
	You are informed that you can allow the app to collect the data of your photos to improve the app.	x	x			x			
	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You can see the third-party apps you connected to your account. You can revoke the connection.			x				x	
	You can delete your account.								x
		3	3	1	0	3	0	1	1
Wish	You are informed that you can allow the app to share your data with Facebook to personalize the ads you see.			x				x	
	You can delete your account.								x
		0	0	1	0	0	0	1	1
Pou	You are informed that you can allow the app to use your data to personalize the ads you see		x				x		
		0	1	0	0	0	1	0	0
PicsArt	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network. You can delete the data that have been collected.	x	x			x			x
	You can see the history of your activities in the app.	x			x				
	You can delete your account.								x
		2	1	0	1	1	0	0	2
MX Player	You are informed about what optional permissions you can grant the app and why they are asked.	x	x						
	You are informed that the app needs access to the device storage to work properly.	x	x						
	You are informed that the app allows its partners to personalize the ads you see according to your data.			x					
	You are informed that the history of your activities is collected. You can see it and delete it completely or partially.	x			x				x
		3	2	1	1	0	0	0	1
Hill Climb Racing	You are informed that you can allow the app to share your advertising Id with its partners to personalize the ads you see.	x		x				x	
		1	0	1	0	0	0	1	0

LIKEE	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You can delete your account.								x
		1	1	0	0	1	0	0	1
Temple Run 2	You are informed about what types of data are collected and how they are used by the app itself to improve the product and by external partners to personalize the ads you see. You can allow the app to collect and share such data for the personalization of ads.	x	x	x		x			
	You can see the specific partners with which the app share data and decide whether to allow their inclusion in the partners list.			x				x	
		1	1	2	0	1	0	1	0
Uber	You are informed that you can allow the app to use the data of your location to improve your experience.	x	x			x			
		1	1	0	0	1	0	0	0
Google Translate	You are informed about what optional permissions you can grant the app and why they are asked.	x	x						
	You are informed that you can allow the app to collect the images you capture with the camera to improve the product.	x	x			x			
	You are informed that the translation history is collected. You can see it and delete it partially or completely.	x			x				x
		3	2	0	1	1	0	0	1
Pinterest	You are informed that the content suggestions are based on the topics you have saved. You can remove the topics you have saved.	x	x			x			x
	You are informed that the content suggestions are based on the topics you said you are interested in. You can change them.	x	x			x			x
	You are informed that the information shared by third party apps to which you have collected your account are used to personalize your experience. You can delete the connection.			x				x	
	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You are informed that you can allow the app to use the information about the websites you visit to personalize your experience.	x	x				x		
	You are informedt that you can allow the app to use the information about your activities to produce analytical reports of the ads performances.	x	x				x		
	You are informed that you can allow the app to use the information shared by external partners to personalize the ads you see.			x				x	
	You are informed that you can allow the app to use the information about your activities int the app to improve the Pinterest ads you see outside the app.	x		x				x	
	You can delete the account and all the associated data								x
		6	5	3	0	3	2	3	3
Opera	You are informed that you can use the Incognito Mode to navigate without allowing the collection of your data.	x		x		x		x	
	You are informed that your experience is personalized according to your topics of interests. You can change them.	x	x		x	x			x

	You can disable cookies					x		x	
	You are informed that you can allow the collection of usage data. You can delete them.	x				x			x
	You can allow external partners to collect data about you and show you personalized ads.			x				x	
	You can delete your browsing data								x
		3	1	2	1	4	0	3	3
Telegram	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network. You can delete the data that have been collected	x	x			x			x
	You are informed that your data are not shared with external partners.			x					
	You can see the list of bots and websites where you have signed up through Telegram and revoke the connection.			x				x	
	You can delete your payment information	x							x
	You can delete your delivery information	x							x
		3	1	2	0	1	0	1	3
B612	You are informed that the app requires access to the camera, storage, microphone and location to work properly.	x							
	You are informed that you can allow the app to access your location data.	x				x			
	You can delete your account.								x
		2	0	0	0	1	0	0	1
Ludo King		0	0	0	0	0	0	0	0
imo	You are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
	You are informed that you can allow the app to access your phone is asked to quickly verify your phone number.	x	x			x			
	You can download your account information	x			x				
	You can delete your account								x
		3	2	0	1	2	0	0	1
Temple Run	You are informed about what types of data are collected and how they are used by the app itself to improve the product and by external partners to personalize the ads you see. You can allow the app to collect and share such data for the personalization of ads.	x	x	x		x			
	You can see the specific partners with which the app share data and decide whether to allow their inclusion in the partners list.			x				x	
		1	1	2	0	1	0	1	0

Adobe Acrobat Reader	You can allow the app to collect usage data to improve the app	x	x			x			
	You can allow the app to collect error logs	x				x			
		2	1	0	0	2	0	0	0
Files by Google	You are informed that the app need access to your files to work properly.	x	x						
	You can see and delete partially or completely your search history.	x			x				x
		2	1	0	1	0	0	0	1
Shazam		0	0	0	0	0	0	0	0
Microsoft SwiftKey Keyboard	You are informed that the app learns your typing style to enable you to type faster.	x	x						
	You can allow the app to learn your favourite emojis to suggest them while typing.	x	x				x		
	You can allow the app to collect usage data to improve the product. You can delete them.	x	x			x			x
		3	3	0	0	1	1	0	1
8 ball	You can allow the app to share your data with its partners to personalize the ads you see			x				x	
		0	0	1	0	0	0	1	0
Mi File Manager	You can delete all the data about your files that have been collected	x							x
		1	0	0	0	0	0	0	1
YouTube Music	You can allow YouTube to collect your search history and use it to personalize your experience. You can see it, together with the details of the specific search, and delete it completely or partially.	x	x		x	x			x
	You can allow YouTube to collect the history of what you watch and use it to personalize your experience. You can see it, together with the details of the specific activity, and delete it completely or partially.	x	x		x	x			x
	You can see the type of data YouTube collects and download them	x			x				
	You can set the periodic elimination of the history of your activities on YouTube.								x

	The app suggests you content according to your tastes and to the context	x	x						
	You can see the list of third-party apps connected to your account. You can revoke the connection.			x				x	
	You can import data from Google Play Music	x				x			
	You can allow the app to use your location to suggest you personalized content.	x	x				x		
	You can choose the artists you like to furtherly personalize the suggestions	x	x		x	x			x
		7	5	1	4	4	1	1	4
Linked In	You can allow the app to use the information of your calendar to personalize your experience and the ads you see	x	x			x			
	You can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network. You can delete the data that have been collected.	x	x			x			x
	You can allow the app to use your demographic information to personalize your experience and the ads you see. You can see them and review them	x	x		x	x			x
	You can see the list of external partners you connected to your account. You can revoke the connection.			x				x	
	The history of your activities in the app is collected. You can see it and delete it completely or partially.	x			x				x
	You can download your data	x			x				
	You can see the topics of interest that LinkedIn has inferred about you, which are used to personalize the ads you see. You can review them.	x	x		x				x
	You can see the data about the remuneration of your jobs that you provided. You can delete them	x			x	x			x
	You can manage the data LinkedIn have saved when you applied for jobs through your LinkedIn account.	x			x				x
	You can allow the app to personalize the ads you see according to the groups you entered	x	x				x		
	You can allow the app to personalize the ads you see according to your education	x	x				x		
	You can allow the app to personalize the ads you see according to your job information	x	x				x		
	You can allow the app to personalize the ads you see according to your employer information	x	x				x		
	You can allow the app to personalize the ads you see according to the websites you visit	x		x				x	
	You can allow the app to personalize the ads you see outside the app according to your LinkedIn information.	x		x				x	
	You can allow the app to personalize the ads you see according to information you shared with external partners.			x				x	
	You can allow external partners to analyse your data for market research.			x				x	
	You can allow the app to share the jobs you are looking for with companies that advertise them.	x		x				x	

	You can allow the app to share your job history with Microsoft Word to customize your CV.	x		x				x	
	You can allow the app to analyse your interactions with the ads you have seen to monitor the performances of the ads.	x	x				x		
	You can delete your account.								x
	You are informed that your search history is collected. You can see it and delete it partially or completely.	x			x				x
		18	9	7	7	4	5	7	8
Zoom	You can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.	x	x			x			
		1	1	0	0	1	0	0	0

Appendix B: Proactive apps details

APP	TRANSPARENCY OR CONTROL FEATURE OFFERED BEFORE BEING ABLE TO ACTUALLY USE THE SERVICE	CHANNEL		STRATEGY		
		PLAY STORE	SERVICE PRESENTATION	INFORMATION ONLY	AUTHORIZATION HEADS-UP	EARLY CONTROL
WhatsApp	In the Play Store page, you are informed that the app needs to access the data in your phonebook to connect you to your contacts in the app's network.	x			x	
	In the service presentation, you are informed that you can allow the app to access to your contacts, pictures and storage in order to restore your personal Cloud backup.		x		x	
		YES	YES	YES	YES	
Facebook	In the service presentation, you are informed that you can allow the app to collect your exact location to personalize your experience.		x		x	
			YES		YES	
Google Chrome	In the service presentation, you are informed that you can allow the app to synchronize the information (password, browsing history, etc.) of your Google Account in order to personalize your experience, the ads you see and other Google Services.		x			x
	In the service presentation, you are informed that you can allow the app to collect diagnostic data to improve the product		x			x
			YES			YES
Messenger	In the service presentation, you are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.		x		x	
	In the service presentation, you are informed that you can allow the app to send and receive SMS through the app.		x		x	
			YES		YES	
Subway	In the service presentation, you are informed that Subway Surfers collects the data of your activities in the app.		x	x		

	In the service presentation, you are informed that Subway Surfers collects additional data to improve the app.		x	x		
	In the service presentation, you are informed that you can allow Subway Surfers to collect and share your advertisement ID with third-party advertisers to personalise the ads you see.		x			x
			YES	YES		YES
Tiktok	In the Play Store page, you are informed that the videos you see are personalized according to what you see, like and share.	x		x		
	In the service presentation, you are informed that you can allow TikTok to use data of your activities in the app to personalize the ads you see.		x			x
		YES	YES	YES		YES
Candy Crush Saga	In the Play Store page, you are informed that the app shares personal data with advertisers to personalize ads.	x		x		
	In the Play Store page, you are informed of your right to forbid the developer to share your personal data with advertisers to personalize ads and invited to contact them through the dedicated page*	x		x		
		YES		YES		
SHAREit	In the service presentation, you are informed that the app needs to access to the apps you have installed on your device, your location data and information about your device to work properly.		x		x	
	In the service presentation, you are informed that the data that the app collects will be moved and treated in China.		x	x		
	In the Play Store page, you are informed that the app will not ask for permissions that are irrelevant to its functionality.	x			x	
	In the Play Store page, you are informed that the app will ask the permission to your Bluetooth settings to discover nearby users more quickly.	x			x	
	In the service presentation, you are informed that the app collects information to personalize your experience and the ads you see.		x	x		
	In the Play Store page, you are informed that the app will ask the permission to your location to help you discover nearby users.	x			x	
		YES	YES	YES	YES	
Netflix	In the Play Store page, you are informed that the more you use Netflix the better the suggestions will be.	x		x		
		YES		YES		

Microsoft Word	In the Play Store page, you are informed that the data generated with the app usage may be accessible to Microsoft and third-party partners.	x		x		
	In the Play Store page, you are informed that the data generated with the app usage may be moved and treated in the United States.	x		x		
		YES		YES		
Hangouts	In the service presentation, you are informed that you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.		x		x	
			YES		YES	
Messages	In the service presentation, you are informed that you can allow the app to send information about your chats to Google to provide an anti-spam filter.		x			x
			YES			YES
Samsung Internet Browser	In the Play Store page, you are informed about what optional permissions you can grant the app and why they are asked.	x			x	
	In the service presentation. you can allow Samsung to collect error logs to improve the product.		x			x
		YES	YES		YES	YES
Microsoft Excel	In the Play Store page, you are informed that the data generated with the app usage may be accessible to Microsoft and third-party partners.	x		x		
	In the Play Store page, you are informed that the data generated with the app usage may be moved and treated in the United States.	x		x		
		YES		YES		
Microsoft PowerpPoint	In the Play Store page, you are informed that the data generated with the app usage may be accessible to Microsoft and third-party partners.	x		x		
	In the Play Store page, you are informed that the data generated with the app usage may be moved and treated in the United States.	x		x		
		YES		YES		

Google Calendar	In the service presentation, you are informed that the data about your position is used to personalize the graphic style of the Agenda.		x	x		
	In the Play Store page, you are informed that the data from Gmail is used to show you events and bookings in the calendar.	x		x		
	In the service presentation, you are informed that you can allow the app to collect data from Gmail to show you events and bookings in the calendar. You can't change the setting in the service presentation, you are only informed that you will be able to do it later in the settings.		x	x		
		YES	YES	YES		
Google Docs	In the Play Store page, you are informed about what optional permissions you can grant the app and why they are asked.	x			x	
		YES			YES	
Samsung Heath	In the service presentation, you are informed that you can allow the app to collect health data.		x			x
	In the service presentation, you are informed that you can allow the app to use your data to personalize your experience		x			x
	In the service presentation, you are informed that you can allow the app to collect your position data		x			x
			YES			YES
Google Keep	In the Play Store page, you are informed about what optional permissions you can grant the app and why they are asked.	x			x	
		YES			YES	
Garena Free Fire	In the service presentation, you are informed of the permissions that must be granted to use the app and why they are needed.		x		x	
			YES		YES	
My Talking Tom	In the service presentation, you are informed that you can allow the app and its partners to collect and analyse your data to personalize the ads you see.		x			x
	In the service presentation, you can see the specific partners with which the app share data, access their privacy policy and decide whether to allow their inclusion in the partners list.		x			x

			YES			YES
Viber Messenger	In the service presentation, you are informed that the content of your chats is not shared		x	x		x
	In the service presentation, you can allow the app to personalize the ads you see according to the links you click.		x			x
	In the service presentation, you can allow the app to personalize the ads you see according to information shared by external partners.		x			x
	In the service presentation, you can allow external partners to save and read information on your device.		x			x
	In the service presentation, you can allow external partners to infer your personal profile to personalize the ads you see.		x			x
	In the service presentation, you can allow external partners to infer your personal profile to personalize the content you watch.		x			x
	In the service presentation, you can allow external partners to monitor the effectiveness of the ads they show you.		x			x
	In the service presentation, you can allow external partners to monitor the effectiveness of the content you watch.		x			x
	In the service presentation, you can allow external partners to use the information they collect about you for market research.		x			x
	In the service presentation, you can allow external partners to use the information they have about you for improving their products		x			x
	In the service presentation, you are informed that external partners aggregate different data sources to combine your information		x	x		
	In the service presentation, you are informed that external partners aggregate data from different devices to combine your information		x	x		
	In the service presentation, you are informed that the app share data with vendors to guarantee security, prevent frauds and debug		x	x		
	In the service presentation, you can allow external partners to read basic information that your device sends by default (e.g. IP Address) to identify it and show you personalized ads		x			x
	In the service presentation, you can allow external partners to create digital IDs to identify and actively track your device		x			x
	In the service presentation, you can see the identity of the external partners and how they use the data		x			x

	shared by the app and you can decide whether to allow their inclusion in the partners list.					
	In the service presentation, you can allow external partners to use your exact location to personalize your experience.		x			x
			YES	YES		YES
Truecaller	In the Play Store page, you are informed that the app does not share information of your phonebook.	x			x	
	In the service presentation, you are informed that the app requires to access your call history, your contact list and SMS in order to work properly.		x		x	
	In the service presentation, you are informed that some data (name, phone number, IP address, etc.) are collected and analysed.		x	x		
	In the service presentation, you are informed that the collected data are used to improve, analyse and personalize the service that is offered.		x	x		
	In the service presentation, you are informed that the collected data are used to adhere to laws and protect users' security.		x	x		
	In the service presentation, you are informed that the collected data are used, after de-identification to generate reports and statistical analysis.		x	x		
	In the service presentation, you can allow the app to collect your data to personalize the ads you see.		x			x
		YES	YES	YES	YES	YES
My Talking Angela	In the service presentation, you can allow the app and its partners to collect and analyse your data to personalize the ads you see.		x			x
	In the service presentation, you can see the specific partners with which the app share data, access their privacy policy and decide whether to allow their inclusion in the partners list.		x			x
			YES			YES
LINE	In the service presentation, you can allow the app to access your phone to collect your phone number and use it to create you an account.		x		x	
	In the Play Store page, you are informed about what optional permissions you can grant the app and why they are asked.	x			x	
		YES	YES		YES	
Temple Run 2	In the service presentation, you are informed about what types of data are collected and how they are used by the app itself to improve the product and by external partners to personalize the ads you see. You can allow the app to collect and share such data for the personalization of ads.		x	x		x

			YES	YES		YES
Google Translate	In the Play Store page, you are informed about what optional permissions you can grant the app and why they are asked.	x			x	
	In the service presentation, you can allow the app to collect the image you capture with the camera to improve the product.		x			x
		YES	YES		YES	YES
Opera	In the Play Store page, you are informed that you can use the Incognito Mode to navigate without allowing the collection of your data.	x		x		
	In the Play Store page, you are informed that your experience is personalized according to your topics of interests.	x		x		
	In the service presentation, you can allow external partners to collect data about you and show you personalized ads.		x			x
		YES	YES	YES		YES
Telegram	In the service presentation, you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.		x		x	
	In the Play Store page, you are informed that your data are not shared with external partners.	x		x		
		YES	YES	YES		
B612	In the service presentation, you are informed that the app requires access to the camera, storage, microphone and location to work properly.		x		x	
		YES	YES		YES	
imo	In the service presentation, you can allow the app to sync the data in your phonebook to connect you to your contacts in the app's network.		x		x	
	In the service presentation, you can allow the app to access your phone to collect your phone number and use it to create you an account.		x		x	
			YES		YES	
Temple Run	In the service presentation, you are informed about what types of data are collected and how they are used by the app itself to improve the product and by external partners to personalize the ads you see. You can allow the app to collect and share such data for the personalization of ads.		x	x		x
			YES	YES		YES
Files by	In the service presentation, you are informed that the access to your files is needed for the app to work properly.		x		x	

			YES		YES	
Microsoft SwiftKey	In the Play Store page, you are informed that the app learns your typing style to enable you to type faster.	x		x		
	In the Play Store page, you are informed that the app learns your favourite emojis to suggest them while typing.	x		x		
	In the service presentation, you can allow the collection and analysis of your usage data to improve the product.		x			x
		YES	YES	YES		YES