International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

New Media and Privacy the Privacy Paradox in the Digital World: I Will Not Disclose My Data. Actually, I Will ... It Depends

Andrea Carignani[a]*, Vanessa Gemmo[b]

[a,b]*IULM University, via Carlo Bo, 1, MILANO, 20143, Italy*
[a]*Email: andrea.carignani@iulm.it*
[b]*Email: vanessa.gemmo@iulm.it*

Abstract

The inconsistency of privacy attitudes and privacy behavior is often referred to as the "privacy paradox". In this study, we analyze the privacy paradox through a methodology that allows investigating user behavior in relation to transferring personal data or not in a real context. Our intention is to investigate privacy as a negotiation by verifying whether the incongruous consumer behavior known as the privacy paradox also occurs in a real and blind context, and how this is affected by the data commoditization trend. The classical methodology in these types of studies is based on questionnaires administered to participants in an experiment and the questions relate to their intention to disclose their personal information in different hypothetical scenarios. In all these types of research, the respondents know they are participating in an experiment without any real gains or losses as a result of their actions. To understand how users behave when facing the disclosure or otherwise of personal data in a real context, we analyzed ex-post data from different digital campaigns through one of the most frequently used data vault platforms. Via this platform, a company can configure a series of user actions by rewarding them for every action with a discount on a product. Through this platform, we therefore had the opportunity to investigate how real users in real contexts manage the exchange of personal data for discounts on one or more products.

Keywords: Privacy; Privacy behavior; Privacy paradox; Decision-making; Privacy concerns; Online privacy; Big Data.

---

* Corresponding author.

1. Introduction

In modern information economies, the decreasing cost of storing digital data has enabled capturing, retaining and analyzing more and more information on individuals. Each and every one of us produces a vast amount of digital information not only in terms of volume, but also variety: SMSs, emails, photos and documents saved to the cloud, social media comments, positioning sensor readings (GPS), online shopping data, online booking data, to name but a few. Indeed, a digital identity denotes the reconstruction of a new identity from our digital tracks that with increasing precision reflect our tastes, our preferences, and our expected behaviors as consumers. Appropriate to point out here is that companies sharing and studying these digital data does not in itself have a negative worth. Increasingly personalized services, the creation of niche products as well as saving time in performing certain activities are just some of the benefits consumers obtain against the voluntary disclosure of their data. Despite these positive returns, several surveys have in fact confirmed that the topic of privacy is a major concern among consumers [1]. A concern that has been justified by a recent study on the privacy management of the 50 most visited websites in the world, which found that most use personal information to customize advertising, but above all that a large number of corporations (Google, Yahoo, Microsoft, and Facebook, amongst others) share the data collected with hundreds of their affiliates. On the one hand, several studies show that consumers are fully aware of the risks of using and disclosing their data to third parties [2] and that their main objective is to preserve and protect their digital identity. On the other hand, consumers constantly behave in ways that contradict these concerns.

The privacy paradox resides precisely in this behavior and is based on viewing privacy as a commodity that that can be traded for financial benefits: privacy still has a social and individual value, albeit not absolute, since it can be assigned a financial value in a cost and benefit calculation at the individual and social level [3]. The basic principle is that if consumers disclose their data, they must obtain a tangible or intangible return. The present research project investigates the phenomenon known as the privacy paradox by introducing a methodological variant: instead of using a questionnaire to study the intention to trade personal information where there are no positive or negative consequences to the responses given by participants, we use an interactive method where the active choice to disclose some personal information to a third party is periodically rewarded with a financial benefit (discount on a product). The need for a methodological variant to study this paradox is an acknowledged and much-debated issue in literature that remains open [4].

Before addressing the privacy paradox, it is appropriate to mention some aspects that allow introducing and understanding the context of reference, namely, the transition from a real identity to a digital identity; the difficulty in identifying, in the digital era, which are personal identifying data and which are not; the transition from the concept of personal privacy to that of information privacy; the distinct European and US views on privacy to obtain a value chain explanation of the processes of collecting and disseminating personal digital data, and the issues related to the value of such data in modern information economies. These introductory chapters focus on a synthesis of the most recent evidence without giving too much space to the debates that have arisen in literature over the years. The intention, as mentioned above, is to provide the reader with a map that enables perceiving the changes taking place that increasingly lead to knowingly and unknowingly managing personal digital data as a trade currency and thus a commodity.

2. The context: from a real identity to a digital identity

Today, individuals have a sort of "double identity": a real identity in the physical world and a digital identity. The amount of digital data that each of us produces, analyzed through new generation IT tools, can provide interested third parties with a coherent image of who we are, what we do, and our preferences as consumers. The phenomenon behind the creation of vast amounts of digital data per capita, referred to as the global data explosion, has its roots in mainly four trends: the social media boom, the Internet of Things, increasing online transactions, and access to digital services and media.

The spread of social media has led not only to increased interactions between people, but also to sharing data such as news, product and service information, demographic data, preferences, images, videos, and geo-localization data. A significant fact: by the end of 2015, a quarter of the world's population will be members of a social network. The Internet of Things (IoT) originated thanks to sensors placed within products, such as home appliances and cars, now capable of connecting themselves to the internet, and by 2015, the production of 75 million devices with a direct internet connection is foreseen. Digital data is also collected whenever a song is purchased on the web, when booking a concert ticket or buying a book: the data is saved and made available for later use. Access to digital services and media has further increased the volume of data generated: faster internet access, lower cost of data storage devices, and the increasing number of mobile devices have led to the growing consumption of digital services, such as YouTube, Spotify and Netflix.

Second, it is not only a matter of data volumes, but also the variety of data collected: SMSs, emails, photos and documents in the cloud, social media comments, positioning sensor readings (GPS), online shopping data, service bookings, audio and video files, instant messages such as WhatsApp, and many more. The digital identity formed thus consists of the set of:

- Individual preferences and interests in terms of consumption, opinions, and interests expressed on the web
- Intrinsic characteristics, such as date of birth, gender, nationality, etc.
- Acquired attributes, such as medical records, residential addresses, or online purchasing records

We are in fact experiencing a change towards a model based on consumer information where individuals are simultaneously consumers and producers of the most valuable asset: their personal data.

The world of web marketing is also changing fast and attempting to integrate the potential of Big Data into planning objectives. The data-driven marketing phenomenon is the practice of using consumer data to achieve and measure marketing objectives. An organization defined as data-driven has learned to use data analysis as part of all its marketing campaigns from conception to analyzing the results, capable of generating one-to-one communications through consumer knowledge, learning each time from consumer responses how to adjust the strategy in an A/B testing cycle, and listening to their customers.

3. Variety and difficulty in distinguishing between identifying and non-identifying personal data

The disclosure of data and personal information is the foundation of any social relationship: consider the amount of personal information exchanged during a chat, a dinner, or any social interaction. The same mechanism also applies to the web, where the information we share serves to weave relationships and structure our communications. However, the information we divulge on the web can be digitized and become persistent, replicable, scalable, searchable, and easily shared. The result is that often the actual audience of our communication or information-sharing may differ from those we intended to reach. This is referred to as context collapse, namely, where a heterogeneous audience exists due to a time and space separation. Put simply, the information we disclose online is available to a potentially wide and unknown audience and, as a consequence, involves a large number of contexts that collapse upon one another. Precisely to deal with context collapse, "circles of friends" have been introduced in some of the most popular social networks to identify and limit the target audience of reference. The information that we disclose, commonly known as personal data, can be defined as "any information related to an identified or identifiable individual" and include:

- The content we create through blogs, photos, videos;
- Our behavioral activities such as online searches and purchases;
- All social data such as contacts, friends, likes, etc.;
- Geo-localization data (GPS, IP);
- Demographic data, such as age, gender, income, political affiliation;
- Official identification data such as financial and health information.

Given the increase in data and the ability to analyze and combine these more and more precisely, it is now difficult to establish the boundary between identifying (name, surname, tax code) and non-identifying data (web searches, online purchases, etc.). The very concept of identifying an individual seems to follow a new logic: for example, can geo-localization data be accurate enough to identify us? If a service provider collects data on the web related to anonymous visitors, which will then be traced back to real users when they buy or subscribe to a service, is it actually getting access to ex-post identifying or non-identifying data? The fact remains that we now have to consider as potentially identifying data not only the single personal data we disclose, but the sum of all the data, including those that at first appear irrelevant. This statement, as emphasized in the introduction, is not intended to alarm, but only to emphasize the existing reality, namely, the potential to identify individuals via modern information and communication technologies.

4. From the personal privacy sphere to 'information privacy'

The concept of privacy can in the first instance be defined as the right to self-determine which information is accessible to whom, and when it needs to be accessible. Another important concept to understand and analyse the privacy paradox is that the privacy boundary is not distinct, but a dynamic negotiation between concealing and disclosing personal information. The ideal level of privacy is achieved when the need for an individual's social interaction and self-revelation is in line with his/her need for information storage. In offline contexts, for example, the outcome of this negotiation depends on the precise communication situation occurring at the time.

In the online world, as previously mentioned, some factors change drastically: the content of communications

increases, is disseminated to multiple users, and digitally recorded and replicated. The personal data disclosure negotiation may vary in accuracy and amount of personal information, creating a number of sub-concepts related to the macro concept of privacy such as: anonymity, secrecy, confidentiality, transparency (see Figure 1).

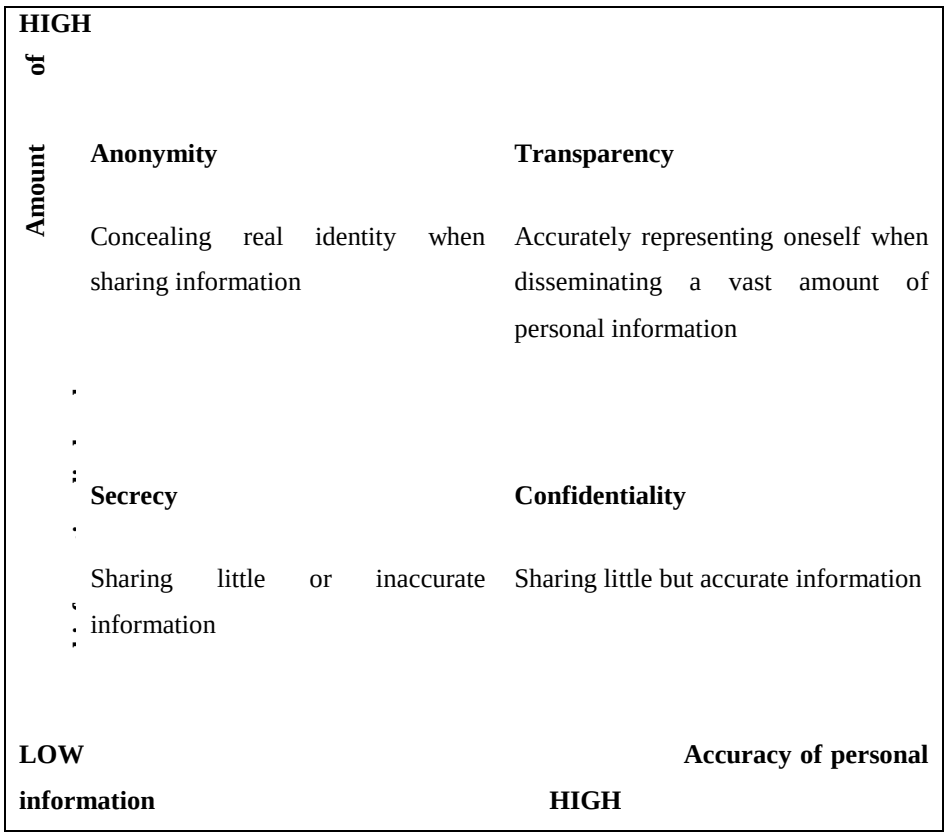

Figure 1: The privacy negotiation matrix

Users have now learnt or are learning to repeatedly deal with the transition between these negotiation states during their interactions with digital media. Consider, for example, each of these terms in relation to social media: while using social media, we have now learnt to move from a state of secrecy to confidentiality by publishing to a circle of friends while excluding, for example, parents or colleagues from a communication. In addition to the concept of privacy as a negotiation, it is also appropriate to summarize here the definition path of the term. A first definition of privacy dating back to 1890 and linked to the personal sphere can be summarized as "the right to be left in peace". Privacy is therefore seen as non-intrusion and privacy of personal thoughts, actions, and property together with the possibility of stopping the amount of information flowing to individuals from others by interrupting it when carrying out personal actions.

The emphasis on the different communication circumstance on the web has led to the definition of information privacy, which has as its focus the privacy of personal data, and is defined as "the right to select which personal information about me is known and by whom"; thus, with a greater emphasis on the concept of controlling information about personal actions. Data disclosure is linked to the concept of recipient as an indispensable communication event in contrast to the concept of solitude.

5. Privacy: human right vs commodity

Generally, in relation to the legislative scope of privacy, two models can be distinguished and compared, namely, the European and American. In essence, the European model deals with privacy as a human right (non-negotiable or debatable) since the end of World War II with the birth of the United Nations and European institutions: privacy is considered a fundamental right to the emergence of democracy (Article 12 of the Universal Declaration of Human Rights and Article 8 of the European Convention of Human Rights). In the American model, privacy is viewed from the perspective of negotiating and analyzing the costs and benefits: as a commodity that can be traded on the market. The American and European models also differ in terms of:

- Legislative approach: the American is sectoral while the European is all-inclusive;
- Regulatory approach: Europe through centralized agencies; the US with the voluntary control of companies sustained by the federal state;
- Rights granted to people: in the US model, none or traditionally only opt-out; in the European model, the rights of inspection, data correction, opt-out and opt-in.

Table 1: A comparison of the American and European models

	US	**Europe**
LEGISLATIVE APPROACH	Sectoral	All-inclusive
REGULATIONS	Sustained voluntary control	Centralised agency
RIGHTS OF INDIVIDUALS	None or opt-out (by sector)	Inspection/Correction/Opt-Out/Opt-In
ROLE OF PRIVACY IN FIRMS	Contractual	Human Rights

Put simply, the legislative pathway took place in three macro phases. In 1955, the European Union Data Protection Directive established that the purpose and means of using personal data should be explicit and there must be a public authority to monitor the privacy issue. Member States have the freedom to apply the Directive (some require opt-in and opt-out, others to certify each single database used). It is also forbidden to export data to countries with no adequate privacy protection measures.

In 2000, the US Safe Harbor Agreement affirmed that US companies wanting to use personal data from Europe must register at the Department of Commerce with annual certification of their business. Companies are called on to develop their privacy policy or to comply with Safe Harbor requirements. The Federal Trade Commission

(FTC) or State agencies have the task of controlling and supervising certain sectors.

In 2013, the European Commission proposed a reform of the 1955 Data Protection Directive. The reform started from the awareness that the twenty-seven Member States applied the rules of the 1955 Directive in different and fragmented ways. The reform introduced some important changes such as: the right to be forgotten (i.e., the possibility that the digital data will be permanently deleted at the individual's request), informed consent that must always be explicit and never implicit, data portability which refers to transferring personal data from one service provider to another. Interesting to note is that these rules also applied to non-European companies if offering a service in Europe.

In 2015, the European Court of Justice ruled that the decision of the European Commission was inadmissible, which considered the protection of personal data of European citizens in the United States as adequate, allowing transfer according to the Safe Harbor agreements. In this way, to transfer data to the United States, all multinationals, European organizations and businesses have to make recourse to other options provided by data protection legislation.

6. Advantages and disadvantages of personal data disclosure for businesses and consumers

If personal data, as shown, are a necessary and sought-after commodity in the current marketplace configuration, it means that both companies and consumers can benefit from their use. For example, for companies, the benefits deriving from consumers' data disclosure include:

- Learning consumer habits from consumers themselves and then developing targeted offers and reducing advertising costs.
- Predicting market trends by studying personal data even at an aggregate and non-personal level allows a better allocation of business resources by decreasing inventory risk and maximizing investments.
- Appropriately discriminating the price in the offer to users.

Conversely, if consumers' personal data were not disclosed and present, there would more entry barriers and less competition (when some companies have the data and no one can obtain them on the market), diminished innovation capacity in the proposed services and products, and a general problem on a social level as occurred in the Canada census case (in 2010, Canada abolished the traditional census questionnaire for privacy reasons, replacing it with a compulsory short form and a second extended non-compulsory form. The percentage of responses to the non-compulsory form steadily declined and affected research, public health activities and policy decisions). The risks of data manipulation by companies largely imply data breaches and the potential loss of credibility and reputation [5]. However, for consumers, the advantages of disclosing personal data range from:

- Saving time in performing certain activities
- Obtaining financial benefits such as discounts
- Intangible benefits such as membership of a social network or personalization and use of online services

- In addition, they may benefit from product deals that would not be developed without knowledge of consumers (niche products).

Doing more and more to not disclose data in the digital world implies exclusion from some services and products, and this is the main cost of non-disclosure of personal data, in addition to the increase in time in performing certain tasks due to the lack of opportunity to shop online, etc. The negative externalities that are greatly emphasized in the disclosure of personal data range from digital identity theft, spam marketing, and financial infringement in the case of financial data theft. The advantages for the public sector in accessing citizens' personal information include the reduction of manual costs for certain transactions and potentially reducing tax evasion.

7. The value chain and personal data use-models

Several actors are involved in the personal data value chain and are worth listing to enable understanding and contextualizing the discourse on privacy and the risk perception of end users. First, personal data can be collected in a variety of ways: voluntarily when consumers share information with third parties by subscribing to a service, signing up to a social network or entering credit card data during an online purchase and so forth. Other data may also be legally observed and recorded, such as navigation data: clicks made on specific site areas or the location of IP addresses, etc. Data can also be derived from recombining the other data types. The value chain path for any data type includes collection, storage and retention, analysis, and use Key actors in the storage and retention stage generally offer services, also collecting personal data as a by-product of their businesses: Internet Service Providers (ISPs), phone providers, government agencies, online social networks, financial institutions, utilities, retailers where purchases are made, and many others. In the analysis and distribution stage, the actors combine different data sources, adding value in terms of profile creation and analytics that can be used on the market. Therefore, this step includes service providers and retailers who use CRM tools rather than business intelligence services or those who manage loyalty programs. This stage also includes data brokers and online advertising companies. The most common uses in the last stage of the value chain refer to companies that purchase personal data packets for marketing activities, but also governments and public administrations for the creation of public utility programs (licenses, social programs, tax management). Regardless of the production sectors, the use of digital data by companies falls into one of the following six categories:

1. Process automation: simplifying and speeding up. An example is previously stored payment and delivery data for goods when purchasing online or suggestions based on preferences.
2. User Enablement: customer self-service as occurs in the banking and telecommunications world. Companies save manual labor with IT solutions and users save time and effort.
3. Personalization: customizing products and services with user data.
4. Enhanced delivery: improved delivery of products and services, such as Amazon drones.
5. Personal data-driven R&D: Procter & Gamble has adopted this approach for some time using the amount of data on the web to test and halve the cost and time of product development.
6. Secondary monetization: sale of personal data to third party.

8. The value of digital data

What is the value of an individual's digital data on the market? Different ways of analyzing this value have been proposed, even if there is no agreement on a common methodology: usually market-based methodologies (observable or derivative) and methodologies based on the individual's assessment of value. Market-based methodologies are divided into market price analyses where data brokers sell and buy personal data, analysis techniques that take as benchmarks the financial results of data records held and, finally, the price of personal data in digital markets. The market price at the data broker level is influenced by the fact that personal data can be resold and used several times, which is why the value at which they are sold does not reflect their actual value, but is an indication of how a copy of such data is valued. Generally, a physical address can be acquired for .50 cents, an ID number for $8 and a driving license number for $3. The analysis of financial results is carried out by dividing the revenue or net income by the number of profiles held. This metric is easy to calculate and is based on public data, but is unfortunately highly inaccurate. By way of an example, a Facebook record is worth around $98 and Twitter record around $110. A third and often forgotten market is the illegal market where credit cards can be found for $0.85-30, access to online accounts for $15-850 and email accounts for $1-20.

Conversely, methodologies based on an individual's assessment refer to the use of questionnaires or economic experiments and specifically attempt to infer the monetary value that a user would pay to protect his/her data. The imprecision of these assessments is in the fact that individuals evaluate the value of their personal data and their privacy differently, and each decision is relative to the context. Three evaluation clusters of the value of an individual's personal data have been identified:

- Top Tier: social security numbers (ID and credit card information) $150-240
- Middle Tier: digital information history (web browsing, location, etc.) $50
- Facts About Us: purchasing history, online advertising click history: $3-6.

Another important indication of the value that an individual allocates to his personal data is how much s/he is willing to spend to protect his/her data: on average, individuals are willing to pay $100 - $120 a year to protect their data.

9. An alternative research approach to the privacy paradox

When interviewed, consumers are aware of and worry about not having control over the information they reveal on the web. An example is the recent Eurobarometer on data protection (March 2015) where respondents stated that they were aware of having partial control (50%) or no control (31%) over information disclosed online and the possibility of correcting, changing or deleting it. Despite this awareness and concern, there is now ample evidence that consumers nevertheless contradict these statements. Different studies show that privacy concern is negatively correlated with the frequency of registering on websites or services reported by interviewed users. Therefore, the reality of the facts with regard to intentions of use on privacy is that consumers constantly disclose their online data. The most effective explanation is that the benefits of disclosure are often immediate

(access to a site, obtaining a discount, etc.) while the risks of such behaviors are either hidden or too distant in the future to be perceived as such, and hence the privacy paradox.

A gap to bridge in research on this issue concerns the fact that studies focus on the intention to disclose personal data in certain situations. Participants know they are taking part in an experiment and therefore do not obtain either real gains or losses as a result of their actions. This present study differs by proposing a methodological variant: instead of studying the intent to trade personal information through a questionnaire, we use an interactive model where the active choice to disseminate some personal information to a third party is from time to time recompensed with a financial benefit.

Our intention in this research project is to investigate privacy as a negotiation by verifying whether the incongruous consumer behavior known as the privacy paradox also occurs in a real context, and how this is affected by the data commoditization trend. The classical methodology in these types of studies is based on questionnaires administered to participants in an experiment and the questions relate to their intention to disclose their personal information in different hypothetical scenarios. In all these types of research, the respondents know they are participating in an experiment without any real gains or losses as a result of their actions.

To understand how users, behave when facing the disclosure or otherwise of personal data in a real context, we analyzed ex-post data from different digital campaigns through one of the most frequently used data vault platforms in Europe. Via this platform, a company can configure a series of user actions by rewarding them for every action with a discount on a product. For example, if wanting a user to watch and comment on advertising or write an opinion on a product and at the end leave his/her email address to be contacted, a path can be configured where when the user completes each of the three actions, s/he receives an additional discount on a selected product. Through this platform, we therefore had the opportunity to investigate how real users in real contexts manage the exchange of personal data for discounts on one or more products.

In particular, we analyzed 150,323 actions of 9 digital campaigns subdivided into six industries: banking, charity, publishing, internet service providers, transport, and utilities. We performed a logistic regression on the extracted data with the users' disclosure or non-disclosure of data as the dependent variable. The independent variables analyzed include gender, age, geographic area, and type of privacy (explicit or implicit consent) up to providing data to a third party or the length and complexity of the data to be inserted. The users' demographic profile is predominantly male from Italy, aged between 26 and 35 years.

An immediate verification of the privacy paradox concerns an aggregate statistic: in 119,897 cases (80%), the users agreed to transfer their data for a discount on a product, while 30,426 (20%) did not agree. This leads us to think that users are inclined to disclose some personal data in respect of a short-term gain. Deepening the analysis, we highlighted the discount to encourage the disclosure of sensitive personal information (email address, phone number, gender, postcode, province, name, house number) and moderately sensitive data (gender, date of birth, and province). The average discount required to obtain sensitive data is 8.12% and 4.99% for moderately sensitive data (see Table 2).

Table 2: The personal data commoditization metrics highlighted by the research

	Average discount rate
Moderately sensitive data	4.99%
Sensitive data	8.12%

Continuing with the data analysis, we considered which variables influence whether or not date is transferred. This analysis conducted by means of a logistic regression in blocks enabled verifying the best explanatory model within a data group. Although we can therefore state that the results explain the analysed data well, they are unable to predict what might occur with new sets of information. However, as this is a new methodological approach to studying privacy commoditization in a real context, we deem these results serve as preliminary guidelines for future studies and generalizations. From the results collected, the factors that influence the decision of whether or not to disclose personal data are:

- Sensitivity of the data request:
  - A non-sensitive data request has a 63 times greater transfer probability with respect to sensitive data
  - A moderately sensitive data request has a 1.9 greater transfer probability with respect to sensitive data
- The form in which the data are requested also affects the parameters:
  - Verified data has a 6.5 greater transfer probability with respect to free text fields.
  - Mixed data has a 6.8 greater transfer probability with respect to free text fields.
- Industry seems to have a weak influence:
  - Data in the banking sector has a 1.6 greater transfer probability with respect to other industries.

While the first and third result can be easily interpreted, the second deserves some clarification. It would appear from the results that the form in which the data are requested influences whether the user transfers the data or not: the form that has the greatest negative effect on data transfer is that of free fields to be compiled one after another. The form that is less affected is that of verified data, namely, not having to fill out a form because the data has previously been provided and requires only confirming their re-transfer. It therefore seems that the compilation time factor is relevant: the more time users must spend in filling in personal data fields the more they become aware of their actions and are therefore less likely to disclose personal information. Even more interesting is what emerges on the factors that do not affect the decision on whether or not to share personal data:

- Type of privacy (explicit consent with a box to tick online, or implicit consent);
- If transfer to a third party is foreseen in the privacy text;
- The presence of a button to skip the request for personal data and continue navigating;
- Gender, age, or region.

10. Conclusions

In this study, we analyze the privacy paradox through a methodology that allows investigating user behavior in

relation to transferring personal data or not in a real context.

The analysis of the results allows verifying that even in a real context, users fall into the privacy paradox: users will probably only consider the immediate benefits (in this case, a discount on a product) without thinking about the future outcomes of their actions. The fact that type of privacy or third-party transfer clauses are among the factors that do not affect the decision to transfer personal data may mean that users do not actually read these and limit themselves to disclosing data to obtain the discount. From this point of view, the reform proposals of the Data Protection Directive of 1955 on data portability and the right to be forgotten would seem coherent and necessary. Privacy awareness interventions (information and education in particular) could certainly mitigate such consumer behaviors. Another element of note of this study is the identification of some personal data commoditization metrics: if it is true that personal data are the currency of the future, real cases should be investigated of the trade value of this currency and the positive and negative externalities of its availability or not in the markets.

In conclusion, it would seem that if users are "captured" by a discount on a product they deem interesting, they have no difficulty in transferring even sensitive personal information. The context in which this transition occurs certainly has an effect, and trust in the companies with which we dialogue is a further element to be considered in future research in this field. In addition, increasing the number of cases under study and the products involved, the discounts provided, and the types of requests made constitute future research avenues that would enhance our knowledge in this sphere.

Bibliography

[1] Fortes, Nuno; Rita, Paulo. “Privacy Concerns And Online Purchasing Behaviour: Towards An Integrated Model”. Ermbe. Vol. 22, Nº 3, pp. 167-176. DOI: 10.1016/j.iedeen.2016.04.002

[2] K. Sheehan,M., Hoy “Dimensions of privacy concern among online consumers”. Journal of Public Policy and Marketing, 19 (2000), pp. 62-73

[3] Acquisti, A. and J. Grossklags. “What can behavioral economics teach us about privacy?” In S. G. C. L. Alessandro Acquisti, Sabrina De Capitani di Vimercati (Ed.), Digital Privacy: Theory, Technologies and Practices, pp. 363–377. Auerbach Publications (Taylor and Francis Group).

[4] Belanger, F., and Crossler, R.E.. “Privacy in the digital age: A review of information privacy research in information systems”. MIS Quarterly, Vol. 35 N. 4, pp. 1017-1041.

[5] Smith, J. (2001) Information privacy and marketing: What the US should (and shouldn't) learn from Europe, California Management Review, Vol 43, No. 2 Winter 2001.

[6] Potzsch, S. (2009) Privacy awareness: A means to solve the privacy paradox? IFIP AICT, 2009.

[7] Smith, H. J., Dinev, T., and Xu, H. (2011). Information privacy research: An interdisciplinary review, MIS Quarterly, Vol.35, No. 4, pp. 989-1015.