The impact of Cookie Consent Notices on user's privacy concerns: an empirical analysis

Tommaso Maria Bellentani

Dissertation written under the supervision of Martin Quinn

Dissertation submitted in partial fulfillment of requirements for the MSc in Management with specialization in Strategy and Entrepreneurship, at the Universidade Católica Portuguesa, 15.06.2020.

Acknowledgments

I acknowledge the support from FCT – Portuguese Foundation of Science and Technology for the project FCT-PTDC/EGE-OGE/27968/2017.

Abstract

Online privacy has become a significant issue in our society with the use of personal information widespread by websites and firms. To regulate this market, the European Union adopted the General Data Protection Regulation to protect online privacy and give back power to users, requiring firms to recover consent before gathering users' personal information. Therefore, websites introduced cookie consent notices that allow users to specify their choice regarding the management of personal data. However, this design can manipulate user's privacy concerns while navigating the website. To find out how, we developed an experiment divided into two steps: before, users displayed a cookie consent notice and, following, they answered to a set of ten questions with different intrusiveness levels, we aimed to measure the correlation between these two phases. We used the platform Amazon Mechanical Turk to gather data building a database of 320 respondents that we tested running random effects panel logistic models. We found out that users displaying a cookie consent notice with pre-ticked choices increase their privacy concerns when they face it without a "reject all" bulk option or when they answer to intrusive questions. Furthermore, we found out that users acting to protect their privacy tend to disclose more intrusive information and that users with a high level of privacy concern disclose less information compared to the others.
Keywords: online privacy, GDPR, banner, AMT, panel analysis, privacy concern, intrusive, bulk option, pre-selected choices, cookies

A privacidade online tornou-se um problema significativo na nossa sociedade com o uso de informações pessoais generalizadas por sites e empresas. Para regular esse mercado, a União Europeia adotou o Regulamento Geral de Proteção de Dados para proteger a privacidade on-line e devolver o poder aos usuários, exigindo que as empresas recuperem o consentimento antes de coletar informações pessoais dos usuários. Portanto, os sites introduziram avisos de consentimento de cookies que permitem aos usuários especificar suas escolhas em relação ao gerenciamento de dados pessoais. No entanto, esse design pode manipular as preocupações com a privacidade do usuário enquanto você navega no site. Para descobrir como, desenvolvemos um experimento dividido em duas etapas: antes, os usuários exibiam um aviso de consentimento de cookies e, a seguir, respondiam a um conjunto de dez perguntas com diferentes níveis de indiscrição, com o objetivo de medir a correlação entre essas duas fases. Utilizamos a plataforma Amazon Mechanical Turk para coletar dados construindo um banco de dados de 320 respondentes que testamos executando uma análise de painel com efeitos aleatórios Logit modelos. Descobrimos que os usuários que exibem um banner pré-marcado aumentam suas preocupações com a privacidade quando enfrentam em um aviso de consentimento de cookie sem uma opção "rejeitar tudo" ou quando respondem a perguntas intrusivas. Ademais, descobrimos que os usuários que agem para proteger sua privacidade tendem a divulgar informações mais intrusivas e que os usuários com um alto nível de preocupação com a privacidade divulgam menos informações em comparação com os outros.
Palavras-chave: privacidade on-line, GDPR, banner, AMT, análise de painel, preocupação com privacidade, intrusivo, opção em massa, opções pré-selecionadas, cookies

Author: Tommaso Maria Bellentani
Title: The impact of cookie consent notices on user's privacy concerns: an empirical analysis

Contents

Acknowledgments ii
Abstract iii
List of Abbreviations v
List of Tables vi

1 Introduction 1
2 Literature Review 3
2.1 Influence of cookie consent banners on privacy concerns 3
3 Hypotheses 5
4 Empirical Strategy 7
4.1 Experimental Framework 7
4.2 Data Collection 8
4.3 Econometric Models 9
5 Results 12
5.1 Overview 12
5.2 Graphical Analysis 16
5.3 Panel Analysis 17
6 General Discussion 23
6.1 Findings 23
6.2 Managerial Implications 24
6.3 Scientific Implications 25
7 Limitations and recommendations for future research 25
8 Bibliography 27
Appendix 30

List of Abbreviations

AMT	Amazon Mechanical Turk
bn1	banner 1 (unticked – no bulk option)
bn2	banner 2 (ticked – no bulk option)
bn3	banner 3 (unticked – bulk option)
bn4	banner 4 (ticked – bulk option)
bulk option	button to reject/accept all cookies in the banner
et al.	et alii
GDPR	General Data Protection Regulation
ticked_banner	banner with all pre-ticked options
ticked_survey	survey with pre-select yes answer to publishing permission options

List of Tables

Table 1: Overview of our research path 7
Table 2: Overview of our relevant variables 12
Table 3: Overview of our database 13
Table 4: Disclosing rate for our set of questions 14
Table 5: Disclosing rate moderated by acceptance of cookies 15
Table 6: Influence of different relevant variables on the publishing rate 16
Table 7: Random Effects Logistic Models to test the banner influence 18
Table 8: Random Effects Logistic Models to test H1a 19
Table 9: Random Effects Logistic Model to test H1b 20
Table 10: Random Effects Logistic Models to test H2 21
Table 11: Random Effects Logistic Models to test H3 22

1 Introduction

Online privacy has become a significant issue with the digitalization of our society. Every day 3.7 billion humans connect to the Internet creating 2.5 quintillion bytes of data, with exponential growth in the last years (Forbes, 2018). The use of this personal information has become widespread by websites and firms, incentivized by web publishers that collect data aiming to develop personalized advertising (Bergemann and Bonatti, 2015).

Different studies quantified as tremendous the value of the online advertising market, proving how online privacy is not only an ethical issue but also a business issue. For instance, Google conducted an experiment where turned off the access to third-party cookies analyzing an average revenue decreased by 52% for web publishers (Ravichandran and Korula, 2019).

A similar impact was analyzed by Johnson et al. (2019) that identified a revenue loss for publishers over 50% when users opt-out from privacy policies and by Beales and Eisenach (2014) that quantified revenue loss over 60% when users disabled cookies.

To regulate personal information use by private firms, the European Union adopted on May 24, 2018, the General Data Protection Regulation (GDPR) to protect online privacy and give back power to users. This regulation enforced the Privacy and Electronic Communications Directive 2002/58/EC, requiring firms to inform users about the use of their data and recovering their consent before being able to gather personal information.

As expected, the introduction of the GDPR improved users' online privacy. The GDPR led approximately 85% of websites to own privacy policies, 62% of which to recover consent before activating cookies (Degeling et al., 2019). As a consequence, the GDPR caused the cost of personalized marketing channels, mainly display ads, to increase (Goldberg et al., 2019).

The GDPR requires firms to recover consent before gathering personal information. For this motivation, websites modified their privacy policies to allow users to specify their choice regarding the management of personal data. However, many studies already pointed out how the design of cookie consent banners can nudge users towards specific privacy choices.

Proved that choice architecture impacts the acceptance of cookies, the next step is to test how such design can also impact user behavior while browsing the website. Therefore, this research paper will investigate the research gap analyzing how a specific banner design can manipulate privacy choices leading users to change the amount of information they share while navigating a webpage.

We developed an experiment divided into two sections to test this research question.

Firstly, we displayed a banner out of a sample of four to analyze the user's interaction (Appendix A). We built the four banners using two different treatment variables. One to change

the default choice between all ticked and all unticked and the other to allow the user to manipulate all the options with only one click thanks to a second button, reducing the cognitive cost.

Secondly, we conducted a survey consisting of personal life questions, both intrusive and not intrusive (Appendix B). Every question had a publishing permission option to analyze the link between the banner displayed before and the willingness to disclose the information. To defeat the bias by default option, we randomized the publishing permission section to be presented both with all ticked options and all unticked options.

We run the experiment using Amazon Mechanical Turk, incentivizing the respondents to participate thanks to 1$ payment. At the end of our experiment, we totalized an amount of 320 respondents, 53% from countries under GDPR, mainly Italy, Germany, and France, and 47% from other countries, mainly the United States of America. All the respondents were under the same condition and incentivized in the same way.

We found out that users displaying a pre-ticked banner increase their privacy concerns when they face it in a cookie consent notice without a "reject all" option or when they answer to intrusive questions. Instead, the effect of a pre-ticked publishing permission button on the acceptance rate is positive, testifying how strong is the default option bias.

Furthermore, users living in countries under GDPR tend to disclose more information compared to others as we suppose they feel more protected while navigating online.

Moreover, we found out that users acting to protect their privacy tend to disclose more intrusive questions, and that users with a high level of privacy concern publish fewer data compared to the others.

These results suggest how banners can impact user behavior while browsing the website, showing the existence of a trade-off between acceptance of cookies and user experience on the website.

This study has implications for online businesses, as specific banners may erode trust between website and users, leading them to disclose less information while navigating.

Our findings are also crucial for websites that incentivize users to contribute online. As banner design manipulates privacy concerns leading to different provisions by users.

Furthermore, security and institutional websites should also be careful with the banners they use as they have the priority to keep user's anxiety low.

Moreover, this work represents a follow up to the academic research on the impact over privacy concerns of factors as perceived control over information, type of question, and default option.

We support these theories with a practical experiment on a new environment, the privacy policies after the GDPR implementation.

The following chapter will analyze these theories developing a literature review related to the research question. The third chapter will introduce hypotheses based on the research gap found during the literature review, followed by a fourth chapter containing the methodology used to investigate these hypotheses. The fifth chapter will be the core of our study, where we will develop graphical analysis followed by panel analysis on our database to test the hypotheses. The sixth chapter will present the general discussion of our experiment, linking the findings to the existing literature to develop scientific and managerial implications. To conclude, in the seventh chapter, we will introduce the limitations of the study and recommendations for future research.

2 Literature Review

In this chapter, this study introduces the literature related to our research question. We analyze how the framework of a cookie consent banner could impact the willingness to disclose personal information during privacy decisions. To find out, we investigate factors as perceived control over information and type of information to comprehend their influence on privacy concerns. Following, we review different behavioral science concepts to understand how they can impact privacy choices, leading to decisions inconsistent with the user's statements.

2.1 Influence of cookie consent banners on privacy concerns

After the implementation of the GDPR, the cookie consent banner framework in Europe diverged from the rest of the world. The GDPR required the introduction of an opt-in model to regulate the banner, differing it from the typical opt-out model of the American banner. The consequences are significant as an opt-in model drastically decreases the acceptance rate of privacy policies (Bellman et al., 2001) with a considerable impact on the revenue (Johnson et al., 2019). However exists a research gap if this negative effect is at least partially compensated by a positive impact on the privacy concerns, leading users to be more predisposed to share personal information while navigating a website.

Choice architecture drastically influences privacy decisions. The way we design the framework impacts users both with cognitive and behavioral biases. Indeed, in-depth knowledge of the different factors influencing privacy choices is fundamental to comprehend how users can react while exposing them to different inputs (Acquisti et al., 2017).

Considering the importance of choice architecture, we expect that the framework of privacy policies can influence the willingness to share personal information. We already know, according to Braunstein et al. (2011), that wording can manipulate answers on surveys as the framework influences user's privacy concerns both with intrusive and not intrusive questions. We expect to find similar results regarding cookie consent banners, with the structure of the notice manipulating user's anxiety and influencing privacy choices.

An essential factor to manipulate user's privacy concerns is perceived control over personal information. When users feel to have the power to control their data, they reduce privacy worries (Miltgen, 2009), positively moderating the intention to share information (Taylor et al., 2009). Perceived control is so important that users disclose more sensitive information when they feel to have control over their data, even if there is a possibility that unknown people will have access to them (Brandimarte et al., 2013).

Another essential factor to influence privacy choices is the type of information that manipulates user's privacy concerns while answering. If users are sensitive to the question, it is unlikely that they will disclose it while answering. However, it is more likely that they will provide the information if they have the power to decide and control it with the presence of an opt-in or opt-out option (Castañeda and Montoro, 2007).

Control over information and type of information are important factors to understand if a user will disclose data while navigating a website. Nonetheless, there is not always consistency between what users say and how they act. Often people state to care about their privacy, but on practice, they finish to make choices inconsistent with their opinion (Athey et al., 2017). Users are interested in protecting their data, but they tend not to do too much to save their privacy (Boerman et al., 2018).

Three factors can explain this privacy paradox. Firstly, people are favorable to share personal information when they have an incentive, accepting to disclose their data if they can gain something. Secondly, navigation costs have an impact on user's privacy choices. People do not act if it is not necessary, also reducing the protection of their online privacy. Thirdly, encouraging information also incentive users to reduce their privacy concerns, leading them to make different decisions to what they state (Athey et al., 2017).

Furthermore, people tend to be lazy, to be uninterested in spending energies to make a cognitive effort. This cognitive cost leads to select default answers (Samuelson and Zeckhauser, 1988), creating a significant divergence in the acceptance rate between showing a banner with an opt-in or opt-out framework (Bellman et al., 2001).

On the other hand, users also tend to act to minimize the effect of cognitive laziness because this creates the feeling of taking control of the situation (Patt and Zeckhauser, 2000).
In general, people tend to make a choice when they have a limited set of options (Iyengar and Lepper, 2001). When this set is broad, users do not make a decision, accepting the status quo, and increasing the importance of default choices (Dean et al., 2017).

3 Hypotheses

The introduction of the GDPR two years ago led to a stricter regulation for cookie consent banners in Europe, requiring active permission to gather data on websites. Utz et al. (2019) already analyzed how banner position, notice content, and type of choice impact the acceptance of cookies. We start by her work to develop further research on the topic. In particular, we focus on the impact of the framework of a cookie consent notice on user's privacy concerns to see how it influences willingness to disclose personal information while navigating on a website.
The goal of this paper is to fill the actual research gap answering to the question: *Does the banner design influence user's willingness to disclose information during the interaction with the website?*
Firstly, displaying two different banners, one with everything pre-unticked and the other with everything pre-ticked, we expect the first banner to grant a higher willingness to disclose personal information. We suppose users will feel safer as the website wants to recover their consent before gathering personal data.
Secondly, we want to test the impact of a bulk option to manipulate privacy decisions. We already know that bulk options lead users to defeat the default option bias as they reduce the cognitive cost (Nouwens et al., 2020). Now, we test that between displaying two banners, one with a "reject all"/"accept all" button and the other without, the latter to influence to share less information. We suppose that users increase privacy concerns during the experiment when they face a banner with a higher cognitive effort to protect personal data.
Furthermore, we expect the banner to have a more substantial impact on sensitive questions because users will be less in comfort to share personal information (Castañeda and Montoro, 2007).
With the first hypothesis, we want to confirm the existence of a correlation between the banner and the willingness to share information. We expect pre-ticked choices in the banner, while moderated by bulk option and question intrusiveness, to impact this correlation.

H1a: Users allow to publish less information in the survey after displaying a banner with pre-ticked choices. Question intrusiveness moderates this correlation.

H1b: Users allow to publish less information in the survey after displaying a banner with pre-ticked choices. A bulk option moderates this correlation.

Considering we already know that perceiving control over privacy decisions creates incentives to share sensitive personal data (Brandimarte et al., 2013). For the second hypothesis, we want to test that users rejecting all the data usages in the banner will allow more intrusive information to be published. In particular, we expect this correlation to exist when the data usages are pre-selected because, in this situation, users take active control of the situation, protecting their online privacy, and feeling more in comfort to disclose intrusive questions.

H2: Users rejecting all the data usages in pre-ticked banners will allow more intrusive information in the survey to be published.

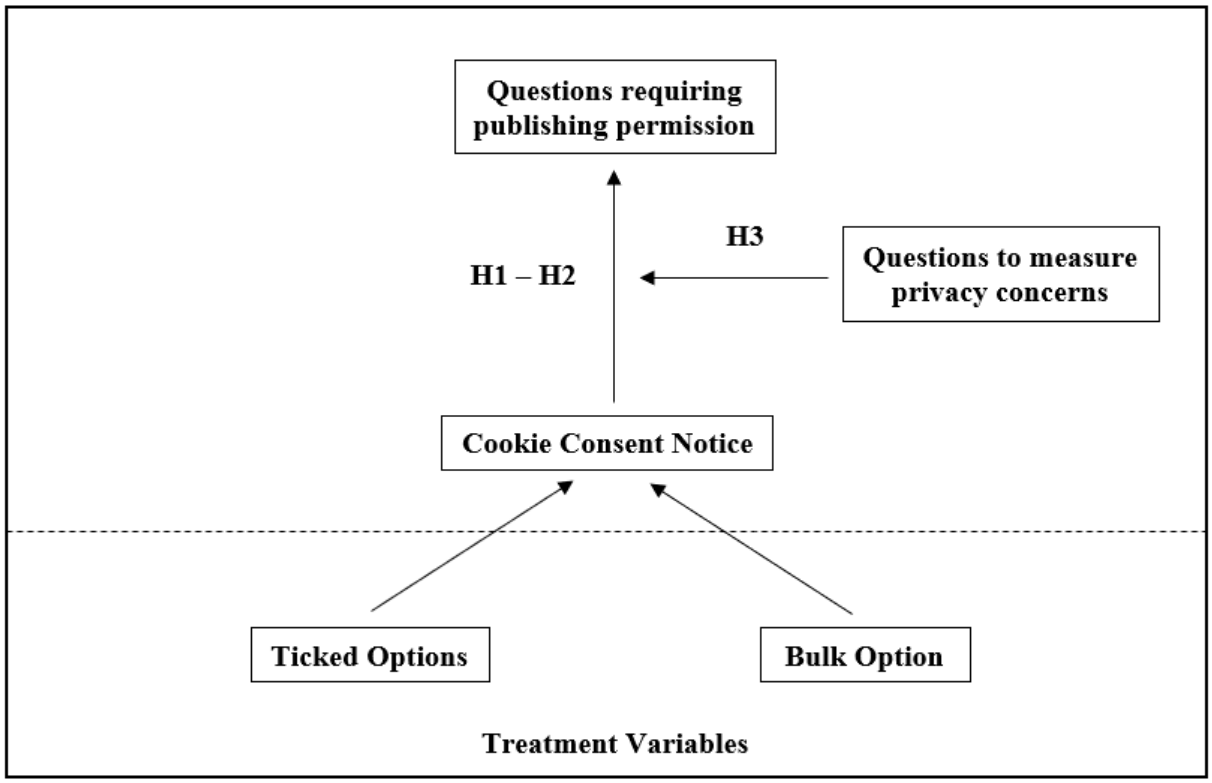
For our last hypothesis, we expect that people with a very high stated level of privacy concern will always avoid disclosing their information, and the banner displayed will not influence their decision. When respondents are very sensitive to the questions, they do not disclose information (Castañeda and Montoro, 2007), protecting their privacy and overcoming behavioral biases. We also expect there will not be a privacy paradox because, in our experiment, we do not have factors as navigation costs and monetary incentives to disclose more information (Athey et al., 2017).

H3: Users with a high level of privacy concern will disclose in the survey less personal information. The banner displayed before will not affect them.

To sum up, in Table 1 below, we summarize our experiment and how it helps us to test our hypotheses. We also identify the connection between our two treatment variables and the cookie consent banner.

Table 1: Overview of our research path

The link between our experiment and the hypotheses



4 Empirical Strategy

In this chapter, the study introduces the methodology of the project. Firstly, we analyze how we built the experiment, dividing it into two phases: the first related to the banner and the second to the survey. Secondly, we highlight under which conditions we opted for this framework and how we gathered data using Amazon Mechanical Turk. To conclude, we introduce the empirical strategy and the models we used to test our hypotheses.

4.1 Experimental Framework

To investigate our hypotheses, we designed an experiment divided into two blocks. In the first one, we built a cookie consent notice with the option to accept or decline three different data types (geolocation, device characteristics, and IP address) and three different data usages (behavioral advertising, website performance, and sharing with third parties).

Using this cookie consent notice, we created two treatment variables to build a total of four banners (Appendix A).

One of the two treatment variables is related to the default choice. Two banners have an opt-in structure with everything ticked off, and the other two an opt-out framework with everything ticked.

The other treatment variable is related to the bulk option. We added a second button next to the submit one to reject all the cookies in one of the two pre-ticked banners, and a second button to accept all the cookies in one of the two unticked banners.

Following, in the second block of the experiment, we built a survey that the respondent proceeded to fill after submitting the cookie consent banner. The core of this second part was a set of ten questions (Appendix B) about ethical behavior on a yes/no framework with different intrusiveness levels. Next to every question, there was an option to allow publishing as anonymous on a Research Bulletin the answer to the question that we used to measure user's privacy concerns. We randomized pre-selection regarding this option.

Brandimarte et al., 2013, has established the set of questions we used. Therefore, we already knew which questions respondents would consider intrusive without further research.

There are two benefits to proceeding in this way. Firstly, when measuring privacy concerns, using the same methodology of a different study permits a direct follow-up, allowing to use high-quality data and to compare the results. Secondly, building a survey to measure user's privacy concerns is complicated and time-consuming, so a reused scale allows saving time to spend on other parts of the work (Preibusch, 2013).

Next to the ethical questions, respondents could also decide if sharing personal demographic information like age, gender, country, educational level, and occupation. At the end of the survey, questions related to privacy concerns were displayed (Appendix C).

4.2 Data Collection

To gather data, we used Amazon Mechanical Turk because results are similar to other methods, but recruitment is more straightforward (Paolacci et al., 2010). Participation in our experiment was voluntary and incentivized by 1$ payment. The respondents were conscious of participating in a survey related to daily life activities, but they did not know about the cookie consent banner to recreate a real-life situation.

We also informed the respondents that the answers would be anonymous and encrypted in a secure server and that only the research team participating in the study would have access to their answers, using the data only for research purposes and for academic documents. An age of at least 18 was required.

Thanks to this experiment, we built a database of 320 respondents. Following, we introduce the different models and variables (Table 2) that we used to test our three hypotheses.

4.3 Econometric Models

Considering the limits of the cross-sectional analysis, as it does not allow us to isolate the impact of every question and its intrusiveness, we opted to work on a longitudinal database to develop a panel study and build random effects logistic models.

As established by Brandimarte et al., 2013, we could develop this type of panel study as we assumed that for every respondent, the publishing permissions are not independents among them, and their correlation is constant between any two answers within the user (Liang and Zeger, 1986).

Therefore we proceed to introduce the models that allow us to measure the probability of an answer to be published under different treatment and moderating variables. All the models are indexed for i={1,…,320} and for j={1,…,10} where *i* identifies the respondent and *j* the question number.

Model 1:

$$p_{ij} = \beta_0 + \beta_1 * ticked\_banner_i + \beta_2 * intrusive_j + \beta_3 * ticked\_banner_i * intrusive_j + \beta_4 * ticked\_survey_i + \beta_5 * EU_i + \beta_6 * no\_bulk\_option_i + \alpha_i + u_{ij}$$

For the first part of our first hypothesis, H1a, we test if users publish less information when they display a banner with pre-ticked default options. Question intrusiveness moderates this correlation.

In Model 1, our dependent variable, denoted by *p*, is the publishing permission for every question and user. It is a dummy variable that takes a value of 1 when the user accepts to publish the information and a value of 0 when the user declines.

To take into consideration question intrusiveness, we use the dummy variable *intrusive*. It has a value of 1 when the question is considered very intrusive and 0 when it is moderately or not at all intrusive. In Appendix B, we listed the intrusiveness levels of the ten questions we used.

Moreover, we use the two dummy variables related to the treatment effects: *ticked_banner* and *no_bulk_option*. Variable *ticked_banner* takes a value of 1 when all the options in the banner are pre-ticked. Variable *no_bulk_option* instead when the “accept all”/”reject all” button is not displayed.

With the interaction term *ticked_banner*intrusive*, we intend to measure if the impact of *ticked_banner* is influenced by answering intrusive questions.

Following, we have a variable *EU* to account for the impact that can have to live in a country under GDPR. The variable has a value of 1 when the respondents live under GDPR, 0 in other cases.

Furthermore, variable *ticked_survey* takes into consideration when the publishing buttons in the survey are pre-ticked, the variable has a value of 1 when users display already ticked buttons and a value of 0 when they do not.

Model 2:

$$p_{ij} = \beta_0 + \beta_1 * ticked\_banner_i + \beta_2 * no\_bulk\_option_i + \beta_3 * ticked\_banner_i * no\_bulk\_option_i + \beta_4 * ticked\_survey_i + \beta_5 * EU_i + \beta_6 * intrusive_j + \alpha_i + u_{ij}$$

For the second part of our first hypothesis, H1b, we test if users allow publishing less information when they display banners with pre-selected choices. Bulk options moderate this correlation.

For this goal, in Model 2, we use as independent variables *ticked_banner* and *no_bulk_option.* It is also displayed their interaction as we want to test if this correlation is more significant when the users face the two treatment effects at the same moment. Variables *ticked_survey*, *EU,* and *intrusive* are also part of the model.

Model 3:

$$p_{ij} = \beta_0 + \beta_1 * reject\_all\_cookies_i + \beta_2 * ticked\_banner_i + \beta_3 * intrusive_j + \beta_4 * reject\_all\_cookies_i * ticked\_banner_i + \beta_5 * reject\_all\_cookies_i * intrusive_j + \beta_6 * ticked\_banner_i * intrusive_j + \beta_7 * reject\_all\_cookes_i * ticked\_banner_i * intrusive_j + \beta_8 * no\_bulk\_option_i + \beta_9 * ticked\_survey_i + \beta_{10} * EU_i + \alpha_i + u_{ij}$$

For the second hypothesis, H2, we test if users rejecting all the data usages allow more intrusive information to be published when options in the banner are pre-selected. To do so, in Model 3, we use variable *reject_all_cookies* that takes a value of 1 when the respondent rejects all data usages in the banner and 0 in all other cases.

Variable *reject_all_cookies* interaction with the variables *ticked_banner* and *intrusive* in Model 3 captures the effect that we want to measure. We also use the variables *no_bulk_option*, *ticked_survey,* and *EU* to complete our model.

Model 4:

$$p_{ij} = \beta_0 + \beta_1 * privacy\_sensitve_i + \beta_2 * intrusive_j + \beta_3 * ticked\_survey_i + \beta_4 * EU_i + \alpha_i + u_{ij}$$

For the last hypothesis, H3, we test if users stating a high level of privacy concern disclose less information, not being influenced by the banner they displayed before.

To do so, in Model 4, we use as main independent variable *privacy_sensitive,* and we test the impact for every banner sub-sample: unticked without a bulk option, ticked without a bulk option, unticked with a bulk option, and ticked with a bulk option. Variables *intrusive*, *ticked_survey,* and *EU* are also part of the model.

The variable *privacy_sensitive* consists of a negative answer to every question in Appendix C, it takes a value of 1 when users reject all the possible incentives that we offered in exchange for the use of their data.

In Table 2 below, we list all the variables we introduced until now. Moreover, we created three dummy variables, *cookie_web*, *cookie_ads*, and *cookie_thirdparties,* that represent the willingness to accept in the banner data usages for website performance, behavioral advertising, and sharing with third parties. These three variables are all linked to the variable *reject_all_cookies,* and they will be used in the next chapter to gather more insights about their connection to the disclosing rate.

We also designed three dummy variables *sensitive_storage*, *sensitive_ads,* and *sensitive_sharing* for the answers to the questions related to privacy preferences (listed in Appendix C), a negative answer related to disclosing personal information for an incentive, will give a value 1 to the variable, 0 otherwise. These three variables all together are linked to *privacy_sensitive*.

Table 2: Overview of our relevant variables

Definition of our variables and the link with the hypotheses

Variable Name	Definition	Hypotheses
p	=1 if the user decides to publish the answer	H1-H2-H3
ticked_banner	=1 if the banner options are pre-ticked	H1-H2-H3
no_bulk_option	=1 if there is not a bulk option in the banner	H1-H2-H3
intrusive	=1 if the survey question is very intrusive	H1-H2-H3
ticked_survey	=1 if publishing permission default option is yes	H1-H2-H3
EU	=1 if the user lives under GDPR	H1-H2-H3
cookie_web	=1 if the user accepts cookies for website performance	H2
cookie_ads	=1 if the user accepts cookies for behavioral ads	H2
cookie_thirdparties	=1 if the user accepts third-party cookies	H2
reject_all_cookies	=1 if the user rejects all data usages	H2
sensitive_storage	=1 if the user gives a negative answer to Q1	H3
sensitive_ads	=1 if the user gives a negative answer to Q2	H3
sensitive_sharing	=1 if the user gives a negative answer to Q3	H3
privacy_sensitive	=1 if the user gives a negative answer to all Qs	H3

5 Results

We proceed to introduce the results of our experiment. Firstly, we give a general overview, showing the demographic characteristics of our sample, the publishing permission rate for our set of 10 questions, and the link between accepting the cookies and disclosing information. Secondly, we investigate deeper in the experiment introducing graphical analysis for the database. In particular, we show how the value of different relevant variables influences the publishing permission rate. To conclude, we analyze the econometric models that we used to validate our hypotheses.

Personal insights related to the results we face enrich the chapter.

5.1 Overview

We start the presentation of our results, dividing our respondents among the different sub-samples related to the banner they display to confirm that there is a balance between the different treatment groups in terms of demographic characteristics. Table 3 below contains these data.

Table 3: Overview of our database

Demographic characteristics of our database

Experimental Condition	Respondents	% Male	% Over 35	% GDPR	% Some College
banner unticked – no bulk option	89	56%	45%	55%	79%
banner ticked – no bulk option	71	70%	49%	56%	74%
banner unticked – bulk option	75	68%	55%	53%	92%
banner ticked – bulk option	85	61%	47%	49%	83%
Total	320	63%	49%	53%	82%

In total, we gathered using the platform AMT 320 respondents, divided in 89 for banner unticked without a bulk option, 71 for banner ticked without a bulk option, 75 for banner unticked with a bulk option, and 85 for banner ticked with a bulk option.

Moreover, gender composition splits our database between 63% male and 37% female. Among the different treatment groups, there is a lack of balance, highlighting that a broader database could be necessary to have a good representation of the population.

Referring to age, 49% of our population is over 35. In this case, randomization worked well as all our four treatment groups have a similar ratio between over and under 35.

Taking into consideration the educational level, respondents of our sample have in 82% of cases at least some college education. The ratio is not the same for every treatment group: for banner unticked with a bulk option is 92%, and for banner ticked without a bulk option is 74%.

Regarding nationality, we face an essential factor for our experiment. 53% of our users live in European countries under GDPR, mainly Italy, Germany, and France, the other 47% are from other countries, mainly the United States of America. The GDPR is a European regulation, so only half of the respondents are used to facing an opt-out banner, leading to expect a difference in impact related to the nationality.

Furthermore, there is a similar ratio among the different treatment groups. Considering that the variable *EU* is part of most of our models, this is very important.

Overall, we can be partially satisfied with our sample as the ratio of the demographic variables is quite similar among the different treatment groups.

Now, to proceed, we introduce the average publishing permission rate of our set of questions.

Table 4: Disclosing rate for our set of questions

Probability of our questions to be disclosed by respondents during the experiment

Questions	Intrusiveness	ticked_survey = 1	ticked_survey = 0	Average
Q1	Low	94%	68%	81%
Q2	High	92%	64%	78%
Q3	High	89%	62%	75%
Q4	High	91%	61%	75%
Q5	Low	93%	63%	77%
Q6	High	94%	60%	76%
Q7	Low	95%	68%	81%
Q8	High	90%	59%	74%
Q9	Low	94%	71%	82%
Q10	Medium	95%	63%	78%

Overall, the average disclosing rate fluctuates between a minimum of 74% to a maximum of 82%. As expected, we found out that questions considered for our research very intrusive, have an average lower percentage rate to be published compared to the other questions. The only exception is caused by Q2 that has a higher publishing rate of Q5, a not intrusive question.

We also identified that there is not a vast difference among the acceptance rate of every question. Users tend to accept or reject the questions depending on their privacy concerns altogether.

We also computed the difference of impact on the disclosing rate between displaying the survey with the publishing permission ticked and unticked. As Table 4 highlights, users disclose, on average, around three more questions if they display the survey with permission options already accepted, testifying a strong impact of the default option bias.

Furthermore, when splitting into the two sub-samples, we still have a difference in terms of disclosing rate between intrusive and not intrusive questions. This difference is more marked when displaying the survey without pre-ticked options; in this case, the minimum is intrusive question Q8 with 59%, and the maximum is not intrusive question Q9 with 71%.

Now, continuing to analyze the disclosing rate of our questions, we test how it is influenced by accepting or rejecting the different cookies.

Table 5: Disclosing rate moderated by acceptance of cookies

Comparing our tools to measure privacy concerns

		BANNERS					
		Accepting cookie_web	**Rejecting cookie_web**	**Accepting cookie_ads**	**Rejecting cookie_ads**	**Accepting cookie_sales**	**Rejecting cookie_sales**
QUESTIONS	**Publishing Permission**						
	Intrusive q	81%	67%	82%	67%	82%	67%
	Not Intrusive q	86%	69%	86%	71%	87%	71%
	Moderating Factors						
	sensitive_storage	25%	33%	26%	32%	25%	32%
	sensitive_ads	54%	70%	53%	71%	53%	70%
	sensitive_sharing	51%	70%	49%	71%	48%	72%

We can analyze in Table 5 that there is a positive correlation between accepting cookies and disclosing more information, both intrusive and not intrusive. Users accepting at least one type of cookies disclose, on average, more than 80% of intrusive questions and more than 85% of not intrusive questions.

Users rejecting cookies disclose, on average, less: 67% for intrusive questions and between 69% and 71% for not intrusive questions.

Furthermore, we also identify that there is no consistency between accepting the cookies and the answers to the questions listed in Appendix C and displayed in Table 5 as *sensitive_storage*, *sensitive_ads,* and *sensitive_sharing*.

Many users accept cookies when stating they would reject them, and, on the other hand, many users reject cookies when stating that they would accept them.

Furthermore, it is interesting to note that the declining rate of cookies is quite similar for the three types, but when asked, users tend to be less sensitive about cookies for website performance.

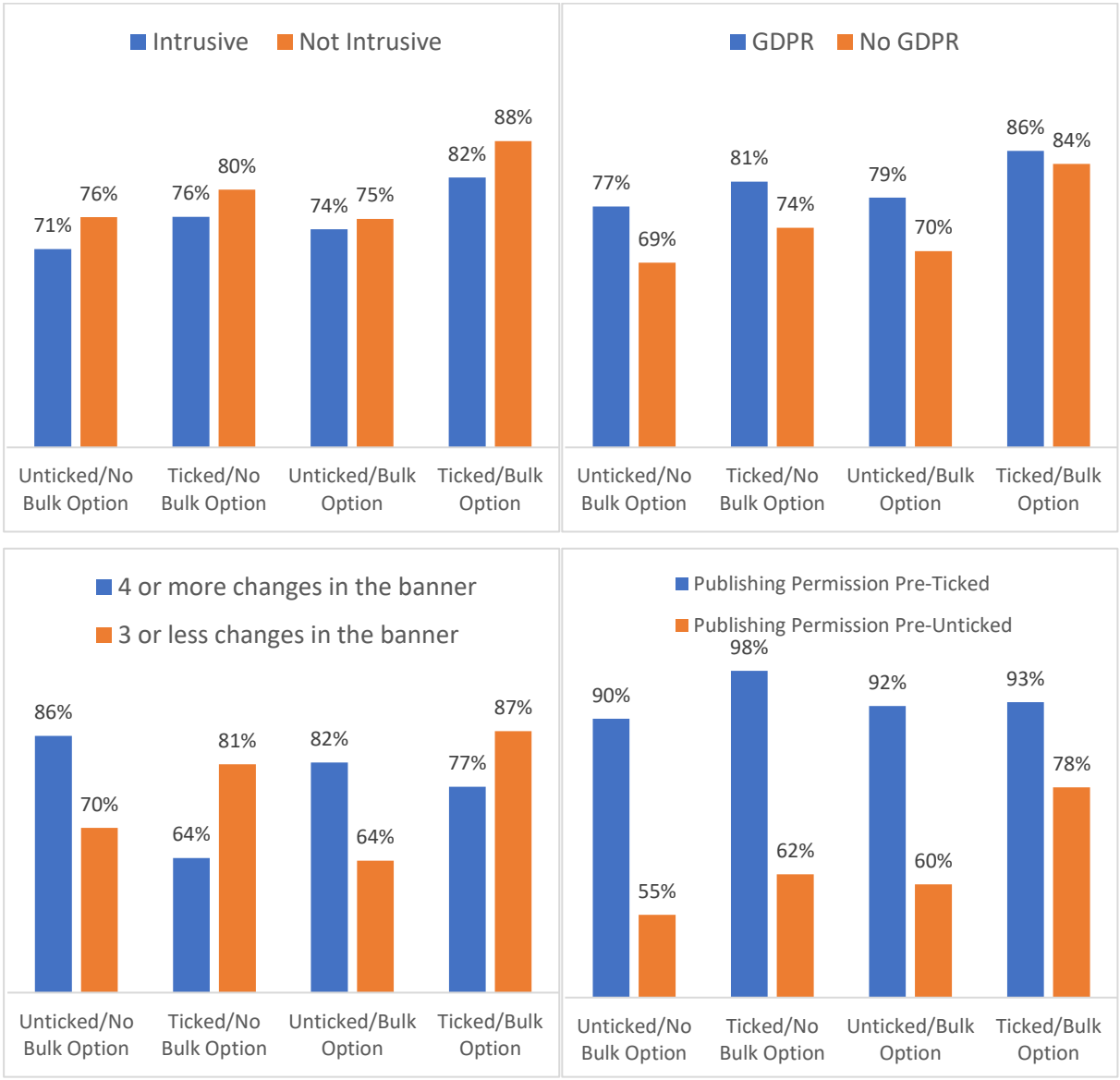
The motivation could be that when respondents accept or reject cookies, they have not a clear idea of what they are accepting/rejecting; they avoid making a cognitive effort. The decision is between accepting and rejecting all, leading respondents to be manipulated by the default option.

5.2 Graphical Analysis

In Table 6 below, we introduce a set of 4 bar charts that we analyze to have further insights about our database. All the graphs display the disclosing rate moderated by the banner and by one of the main variables related to the experiment.

Table 6: Influence of different relevant variables on the publishing rate

User's publishing probability moderated by different relevant variables



The first bar chart highlights that users disclose, on average, less information if they are answering intrusive questions; this is consistent for every banner. Furthermore, the impact seems to be strong in every case except after displaying an unticked with a bulk option banner. Considering this is the banner with the lower cognitive effort to protect personal privacy, it

could suggest that users feel in comfort to share intrusive questions at the same level of the other questions when the cognitive cost is low. However, the average disclosing rate of this banner is lower than the one pre-ticked with the "reject all" button.

This latter effect is fascinating because it highlights that users feel safer to disclose information when they face a pre-ticked banner with a bulk option compared to face that banner directly unticked.

The second bar chart instead shows how, on average, users living in countries under GDPR disclose more information, suggesting that people living in Europe feel more in comfort to disclose. We suppose because they have strict laws protecting their data and their privacy online.

Moreover, it is interesting to analyze how different is the average disclosing rate for users not living in GDPR countries when they face the banner pre-ticked with a bulk option compared to the others. This fact highlights that users living outside countries under GDPR drive the effect of being more manipulated on reducing privacy concerns by adding the "reject all" option compared to directly displaying the banner unticked.

The third bar chart analyzes if users taking control of the situation and changing many options in the banner disclose more information compared to the others. The results show that users changing at least four options publish more data in unticked banners and fewer data in pre-ticked banners. This fact is consistent with Table 5 as it confirms that users accepting cookies share more data and users rejecting them disclose less. The next step is to understand if our second hypothesis, H2, is valid, and users disclose more intrusive data when they reject cookies, being in contrast with the results of this graph and testifying a behavioral bias.

To conclude the graphical analysis, the fourth bar chart shows a strong impact of the default option on the disclosing rate. Users that display the publishing permission options on the survey already ticked share more information. This difference tends to be less significant after displaying the banner pre-ticked with a "reject all" button.

5.3 Panel Analysis

For our panel analysis, we decided to use random effects models after running a Durbin-Wu-Hausman test that showed a higher efficiency compared to fixed effects models. Further details about this test are available in Appendix D.

Considering the binary nature of our dependent variable, we also decided on a logistic regression instead of a linear one. For this motivation, we highlight that we are not able to measure the impact of our variables, but only to understand the direction, if positive or negative.

Moreover, we are not able to display the coefficient of determination, F-statistic, and average marginal effects of our models for limits related to the tool used for computation.
Starting the panel analysis, we display a model to have an overview of the banner influence on the disclosing rate.

Table 7: Random Effects Logistic Models to test the banner influence

The impact of banners on the disclosing rate

	Dependent variable:
	p
bn2 (ticked – no bulk option)	3.837***
	(0.480)
bn3 (unticked – bulk option)	3.952***
	(0.463)
bn4 (ticked – bulk option)	6.267***
	(0.556)
ticked_survey	6.310***
	(0.473)
intrusive	-1.488***
	(0.230)
EU	2.660***
	(0.334)
constant	-0.771**
	(0.372)
Database	all
Observations	3200
Note:	*p<0.1, **p<0.05, ***p<0.01

In Table 7, all the variables of our database are significant. In particular, we analyze how both pre-ticked choices and bulk options have an average positive impact on the disclosing rate. This effect is more substantial when they are both on the cookie consent notice as the coefficient of variable *bn4* shows.
All the banners displayed in the model (ticked without a bulk option, unticked with a bulk option, and ticked with a bulk option) have an average positive impact on the publishing permission compared to the banner unticked without a bulk option.
Users reduce privacy concerns after displaying a banner with a “reject all”/ “accept all” option as this reduces the cognitive effort to protect their privacy. In the same way, a pre-ticked banner leads users to share more data while answering the survey.
Moreover, users increase their privacy concerns when they face sensitive questions disclosing fewer of them compared to the other questions; this is captured by variable *intrusive*.

Consistently with graphical analysis and Table 4, users disclose more information when they display a survey with pre-selected publishing permission options, captured by variable *ticked_survey.*

Finally, users living in countries under GDPR disclose more data as variable *EU* shows.

Finished the overview, we now test H1a and H1b. Differently from Table 7, we isolate the treatment effect of displaying a pre-ticked banner, captured by variable *ticked_banner*, to analyze it more in detail.

Table 8: Random Effects Logistic Models to test H1a

The impact of pre-ticked banners on the disclosing rate, moderated by question intrusiveness

	Dependent variable:				
	p	p	p	p	p
ticked_banner	0.687*	-0.337	4.257***	6.403***	2.981***
	(0.393)	(0.462)	(0.623)	(1.561)	(0.419)
intrusive	-1.175***	-1.592***	-0.687	-1.231*	-1.212***
	(0.304)	(0.413)	(0.486)	(0.632)	(0.355)
EU	2.577***	-0.138	1.880***	3.700***	1.562***
	(0.370)	(0.458)	(0.403)	(1.060)	(0.299)
ticked_survey	6.361***	7.546***	2.873***		
	(0.494)	(0.944)	(0.441)		
no_bulk_option	-0.618**			-0.823	-2.737***
	(0.306)			(0.827)	(0.330)
ticked_banner:intrusive	-0.863*	0.141	-1.270*	-3.641**	-0.217
	(0.472)	(0.615)	(0.654)	(1.466)	(0.492)
constant	2.789***	2.594***	3.549***	10.903***	3.819***
	(0.355)	(0.481)	(0.538)	(1.672)	(0.443)
Database	all	no_bulk_option = 1	no_bulk_option = 0	ticked_survey = 1	ticked_survey = 0
Observations	3200	1600	1600	1520	1680
Note:					*p<0.1, **p<0.05, ***p<0.01

Table 8 uses the strategy laid out in Model 1 and introduced in chapter 4.3 to test hypothesis H1a.

The first column analyzes the whole database, while the other four analyze the sub-samples created fixing the effect of the two other treatment variables: *no_bulk_option* and *ticked_survey*.

Overall, we have consistent results for all the models. The effect of displaying a pre-ticked banner is always positive and significant except for the sub-sample of users that displayed the banner without a bulk option. In this case, displaying a pre-ticked banner decreases the disclosing rate. This last finding supports the second part of our first hypothesis, H1b.

Furthermore, in four of our five models, users disclose less information when they answer to intrusive questions, and they share even less if before they displayed a pre-ticked banner, as variable *ticked_banner:intrusive* shows.

Based on these findings, we can **validate the first part of our first hypothesis, H1a.** Displaying a pre-ticked banner has a positive impact on the disclosing rate, but question intrusiveness negatively moderates this effect. We suppose that it is not enough alone to display a pre-ticked banner to raise the privacy concerns consistently, but it is necessary also a second tool.

We try to gather more information continuing to test the impact of a pre-ticked banner. This time we moderate the treatment effect by the absence of a bulk option.

Table 9: Random Effects Logistic Model to test H1b

The impact of pre-ticked banners on the disclosing rate, moderated by bulk option

	Dependent variable:
	p
ticked_banner	1.489***
	(0.491)
no_bulk_option	-2.093***
	(0.364)
EU	1.378***
	(0.292)
ticked_survey	7.788***
	(0.540)
intrusive	-1.537***
	(0.237)
ticked_banner:no_bulk_option	-3.328***
	(0.636)
constant	3.443***
	(0.393)
Database	all
Observations	3200
Note:	*p<0.1, **p<0.05, ***p<0.01

Table 9 uses the strategy laid out in Model 2 and introduced in chapter 4.3 to test hypothesis H1b.

On average, users disclose less information when they display a banner without a bulk option, captured by variable *no_bulk_option*. The absence of this second button on the banner increases the cognitive cost leading users to raise their privacy concerns and, as a consequence, disclosing less information. This effect is even more substantial when respondents displayed a pre-ticked banner before answering to the questions as variable *ticked_banner:no_bulk_option* shows.

Based on these findings, we can **validate the second part of our first hypothesis, H1b**.

One interpretation about the impact of displaying a pre-ticked banner on the disclosing rate could be that users displaying everything ticked in the banner feel the need to emulate the same situation in the survey to arrive at the end of the experiment. This fact could explain the positive impact of the treatment effect.

Nonetheless, displaying another factor to manipulate privacy concerns as a bulk option or an intrusive question defeats this behavioral bias. In these situations, a pre-ticked banner decreases the disclosing rate.

Table 10: Random Effects Logistic Models to test H2

The impact of rejecting all cookies on the disclosing rate for pre-ticked banners

	Dependent variable:		
	p	p	p
reject_all_cookies	-3.507***	-3.598***	-2.116***
	(0.810)	(0.677)	(0.613)
intrusive	-2.062***		-1.353***
	(0.391)		(0.455)
ticked_survey	6.592***	8.848***	7.492***
	(0.811)	(0.888)	(0.606)
EU	2.540***	1.576***	1.641***
	(0.513)	(0.434)	(0.351)
no_bulk_option	0.281	0.539	-0.006
	(0.449)	(0.451)	(0.379)
ticked_banner		-0.777	0.616
		(0.538)	(0.502)
reject_all_cookies:intrusive	1.364		0.141
	(0.930)		(0.629)
reject_all_cookies:ticked_banner		0.699	-1.401
		(1.034)	(1.098)
intrusive:ticked_banner			-0.769
			(0.583)
reject_all_cookies:ticked_banner:intrusive			1.340
			(1.090)
constant	3.481***	3.330***	3.418***
	(0.586)	(0.563)	(0.474)
Database	ticked_banner = 1	intrusive = 1	all
Observations	1560	1600	3200
Note:			*p<0.1, **p<0.05, ***p<0.01

Table 10 uses the strategy laid out in Model 3 and introduced in chapter 4.3 to test hypothesis H2. We test how users displaying a pre-ticked banner and rejecting all the data usages react to intrusive questions.

Table 10 highlights how, on average, users rejecting all the data usages disclose less information, but they share more intrusive information when the banner displayed is pre-ticked. The

interaction term *reject_all_cookies:intrusive:ticked_banner* captures this effect. This term is positive, with the probability of rejecting the null hypothesis near to 79%.

This fact shows that taking control over the situation and acting to protect personal privacy leads to be in comfort to disclose intrusive data, **validating our second hypothesis, H2.**

Table 11: Random Effects Logistic Models to test H3

The impact of banners on the disclosing rate for users with a high level of privacy concern

	Dependent variable:				
	p	p	p	p	p
privacy_sensitive	-5.336***	0.286	-6.395***	-7.060***	-4.891***
	(0.536)	(0.528)	(1.035)	(1.424)	(1.256)
intrusive	-1.512***	-1.840***	-1.668***	-0.642	-2.170***
	(0.234)	(0.481)	(0.527)	(0.472)	(0.500)
ticked_survey	6.247***	2.906***	10.736***	3.171***	9.731***
	(0.478)	(0.612)	(1.561)	(0.652)	(1.600)
EU	3.132***	3.480***	5.273***	2.387***	7.924***
	(0.437)	(0.673)	(1.015)	(0.695)	(1.470)
constant	3.191***	1.846***	3.539***	3.624***	3.491***
	(0.336)	(0.549)	(0.669)	(0.631)	(0.714)
Database	all	banner 1 unticked no bulk option	banner 2 ticked no bulk option	banner 3 unticked bulk option	banner 4 ticked bulk option
Observations	3200	890	710	750	850
Note:					*p<0.1, **p<0.05, ***p<0.01

To conclude, Table 11 uses the strategy laid out in Model 4 and introduced in chapter 4.3 to test hypothesis H3. We test if users stating a high level of privacy concern disclose less information, not being influenced by the banner they displayed before.

To measure user's privacy concerns, in the survey, we asked to answer three questions (Appendix C) where users were required to decide if they would accept an incentive to disclose more data. We assigned to users rejecting every incentive a high level of privacy concern that we captured in our models using the variable *privacy_sensitive*.

Table 11 shows that, on average, users stating a high level of privacy concern disclose less information when they displayed before the banner ticked without a bulk option, unticked with a bulk option, or ticked with a bulk option. The only case in which users very sensitive disclose as the others, it is after displaying the banner unticked without a bulk option for which the variable is not significant.

Therefore, we can say that, in most cases, users with a high level of privacy concern share fewer data compared to the others. Based on these insights, **our third hypothesis**, **H3, is partially validated**.

6 General Discussion

In this chapter, we proceed to discuss our results, developing scientific and managerial implications related to the research. In particular, we refer to managers and web developers to suggest how they may display cookie consent banners on their webpages to improve managerial results. Furthermore, we link our experiment to the actual literature to discuss how our study impacts different theories.

6.1 Findings

We started this research to investigate if a cookie consent notice can manipulate user's privacy concerns while navigating online, and, thanks to the methodology we built, this study developed different insights filling part of the actual literature gap.

To sum up, we found out that users disclose more information when they face a banner with pre-selected options, we suppose because they face the behavioral bias to imitate in the survey what they saw in the banner. This effect is driven by users that make few changes in the banner as users are subject to this bias when they have privacy concerns low, testified by not acting to reject cookies.

The effect of a pre-ticked banner is negatively moderated by the presence of a "reject all" button and by question intrusiveness, highlighting how pre-selected choices are not enough alone to raise user's worries. However, they contribute if supported by other factors.

Arising privacy concerns lead users to defeat the behavioral bias related to imitating in the survey what displayed in the banner and to act to protect their privacy.

Furthermore, the presence of a bulk option to manipulate all together the cookies decreases user's worries leading them to feel protected to disclose more information. The fact that pre-ticked choices drive this effect proves that the impact of a second button is more substantial in situations where the perceived privacy concerns are considerable. Users give importance to tools related to trust and security when they feel not safe.

Besides, our graphical analysis showed that users not living in countries under GDPR are drastically more influenced by adding a "reject all" option compared to an "accept all" option to reduce the privacy concerns. Instead, users living in countries under GDPR are influenced similarly by adding one of the two buttons to the banner.

This study also found out that users disclose less information when they answer intrusive questions, and they publish more data if they display a pre-selected survey, the default option bias causes this latter effect.

Following, we tested the impact of perceived control over information on the disclosing rate, and we found out that users making an action to reject cookies tend to publish more intrusive information as they feel safe after they acted to protect their privacy.

Moreover, we also tested how users very focused on protecting their privacy react to the banners, and we found out that, in most cases, they are not influenced by them, disclosing less information compared to the other users.

These are the results we reached with our experiment. We now proceed with the managerial and scientific implications related to these findings.

6.2 Managerial Implications

This study has substantial implications for managers and developers. It suggests that the design of cookie consent banners has a tremendous impact on user's choices while browsing a website and highlights its importance to improve managerial results.

This study shows that cognitive costs and default choices alter the privacy concerns, therefore exists a trade-off between accepting cookies and keep user's anxiety low. Different tools used to convince users to accept more cookies have negative consequences on the privacy worries. Arising privacy concerns could impact user's interaction on the website diminishing the capacity to target and leading to less activity on the page.

Moreover, this study highlights that it is crucial to focus not only on the single banner but on the whole picture. We faced treatment effects that alone have a positive impact on the disclosing rate, but that, together with other factors, influence in a negative way the privacy concerns. Therefore, managers and developers should consider every aspect of their website to avoid to arise users' anxiety consistently.

Furthermore, this study found out a trade-off related to perceived control over information. We tested that users disclose at the same time more intrusive information and less not intrusive information when they act to protect their privacy.

All these insights highlight that managers and developers should opt for specific design based on the type of data that maximizes their profit. Depending on the website business, it appears very important to design banners correctly.

Security and institutional websites should focus on keeping user's privacy concerns low; therefore, we suggest banners unticked with a bulk option.

E-commerce websites should display banners with a bulk option to reduce cognitive effort, leading users to accept more cookies.

Moreover, websites that need to recover intrusive information should instead opt for banners that lead users to perceive high control over their information. These websites should accept a reduction over the acceptance of cookies in exchange for a higher disclosing rate, as many users would feel safe to share sensitive data only after they acted to protect their privacy.

6.3 Scientific Implications

We tested different theories and studies during our experiment to be able to confirm them in a new environment.

Firstly, pre-selected choices resulted in having a massive impact on every aspect of our experiment.

In the survey, publishing options already ticked lead users to share, on average, definitely more information.

In the banner, pre-ticked options appeared to lead to a behavioral bias linked to repeat in the survey, the pre-condition of the banner.

Secondly, we also identified how bulk options are an essential factor in reducing respondents' privacy concerns. When users face banners with an "accept all"/"reject all" button tend to disclose more information. Furthermore, bulk options lead to reduce cognitive costs related to make an action.

Thirdly, we tested perceived control over information, measuring a positive correlation with the disclosing rate of sensitive information. Users displaying an opt-out banner and rejecting all the data usages disclosed more intrusive information compared to all other respondents. This effect is connected to a trade-off, as it also leads to disclose, overall, less information.

Fourthly, we also tested a negative impact of question sensitiveness on privacy concerns. Users facing intrusive questions or sensitive situations disclosed less data, trying to protect their data.

All these factors lead us to confirm the importance of choice architecture. Pre-ticked options and bulk options have an impact not only on accepting cookies but also on user experience while navigating the webpage.

7 Limitations and recommendations for future research

We had to accept different limitations to be able to run the experiment.

Firstly, a survey is not a website; therefore, the influence of a cookie consent banner can change while navigating online compared to our environment. Privacy concern manipulation is

something complex to measure, and so we cannot know if our respondents would act in the same way on a webpage.

Furthermore, trustworthiness is an essential factor in keeping privacy concerns low. User behavior can change drastically after displaying a cookie consent notice if visualized on a website visited on a daily routine or joined for the first time. With our experiment, we were able to simulate only the situation in which users enter a webpage for the first time.

Connected to this, we recreated only in part a real-life situation in our study. Users were paid to participate and so interested in arriving at the end of the survey. We could not measure how many would just leave without an incentive to proceed.

Moreover, we were not able to go deeper into the analysis of the differences between countries with and without GDPR and, in particular, among different countries under GDPR. Not enough respondents in our database caused this limit.

Considering these limitations, we suggest running a similar experiment on a website to be able to test on a real-life situation. An element that would be interesting to evaluate it is trustworthiness. To analyze the difference of impact between loyal users and new users, between who is navigating the website for the first time and who visits it daily.

Furthermore, there are other different factors related to the banner that could manipulate privacy concerns and that we did not test. For example, we suggest testing if the text introduction of the cookie consent notice has an impact on it.

Moreover, we think that policy transparency could be an essential factor to manipulate user's anxiety, and we suggest to test it in future research.

We hope the results of this study can be a solid basis for who will come next and will investigate in this fascinating field.

8 Bibliography

Acquisti, A. Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y. and Wilson, S. 2017. 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online'. *ACM Computing Surveys* 50 (3): 44:1–44:41.

Athey, S., Catalini, C. and Tucker, C. 2018. 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk'. SSRN Scholarly Paper ID 2916489. Rochester, NY: Social Science Research Network.

Beales, H. and Eisenach, J. A. 2014. 'An Empirical Analysis of the Value of Information Sharing in the Market for Online Content'. SSRN Scholarly Paper ID 2421405. Rochester, NY: Social Science Research Network.

Bellman, S., Johnson, E. J. and Lohse, G. 2001. 'To Opt-in or Opt-out? It Depends on the Question'. *Commun. ACM* 44 (February): 25–27.

Bergemann, D. and Bonatti, A. 2015. 'Selling Cookies'. *American Economic Journal: Microeconomics* 7 (3): 259–94.

Boerman, S. C., Kruikemeier, S. and Borgesius, F. J. Z. 2018. 'Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data'. *Communication Research*, October, 0093650218800915.

Brandimarte, L., Acquisti, A. and Loewenstein, G. 2013. 'Misplaced Confidences: Privacy and the Control Paradox'. *Social Psychological and Personality Science* 4 (3): 340–47.

Braunstein, A., Granka, L. and Staddon, J. 2011. 'Indirect Content Privacy Surveys: Measuring Privacy without Asking about It'. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 1–14. SOUPS '11. Pittsburgh, Pennsylvania: Association for Computing Machinery.

Castañeda, J.A. and Montoro, F.J. 2007. 'The Effect of Internet General Privacy Concern on Customer Behavior'. *Electronic Commerce Research* 7 (2): 117–41.

Dean, M., Kıbrıs, Ö. and Masatlioglu, Y. 2017. 'Limited Attention and Status Quo Bias'. *Journal of Economic Theory* 169 (May): 93–127.

Degelin, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. and Holz, T. 2019. 'We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy'. *Proceedings 2019 Network and Distributed System Security Symposium*.

Goldberg, S., Johnson, G. and Shriver, S. 2019. 'Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic & E-Commerce Outcomes'. SSRN Scholarly Paper ID 3421731. Rochester, NY: Social Science Research Network.

Iyengar, S. and Lepper, M. 2001. 'When Choice Is Demotivating: Can One Desire Too Much of a Good Thing?' *Journal of Personality and Social Psychology* 79 (January): 995–1006.

Johnson, E.J., Bellman, S. and Lohse, G.L. 2019. 'Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?' SSRN Scholarly Paper ID 3020503. Rochester, NY: Social Science Research Network.

Liang, K. and Zeger, S. 1986. 'Longitudinal Data Analysis Using Generalized Linear Models'. *Biometrika* 73 (1): 13–22.

Marr, B. 2018. 'How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read'. Forbes. Accessed May 27, 2020. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/.

Miltgen, C. L. 2009. 'Online Consumer Privacy Concern and Willingness to Provide Personal Data on the Internet'. *International Journal of Networking and Virtual Organisations - IJNVO* 6 (August).

Nouwens, M., Liccardi, I., Veale, M., Karger, D. and Kagal, L. 2020. 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence'. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, April, 1–13.

Paolacci, G., Chandler, J. and Ipeirotis, P. 2010. 'Running Experiments on Amazon Mechanical Turk'. *Judgment and Decision Making* 5 (5): 9.

Patt, A., and Zeckhauser, R. 2000. 'Action Bias and Environmental Decisions'. *Journal of Risk and Uncertainty* 21 (1): 45–72.

Preibusch, S. 2013. 'Guide to Measuring Privacy Concern: Review of Survey and Observational Instruments'. *International Journal of Human-Computer Studies* 71 (12): 1133–43.

Ravichandran, D. and Korula, N. (2019). Effect of disabling third-party cookies on publisher revenue. *Google Report*. August 27, 2019.

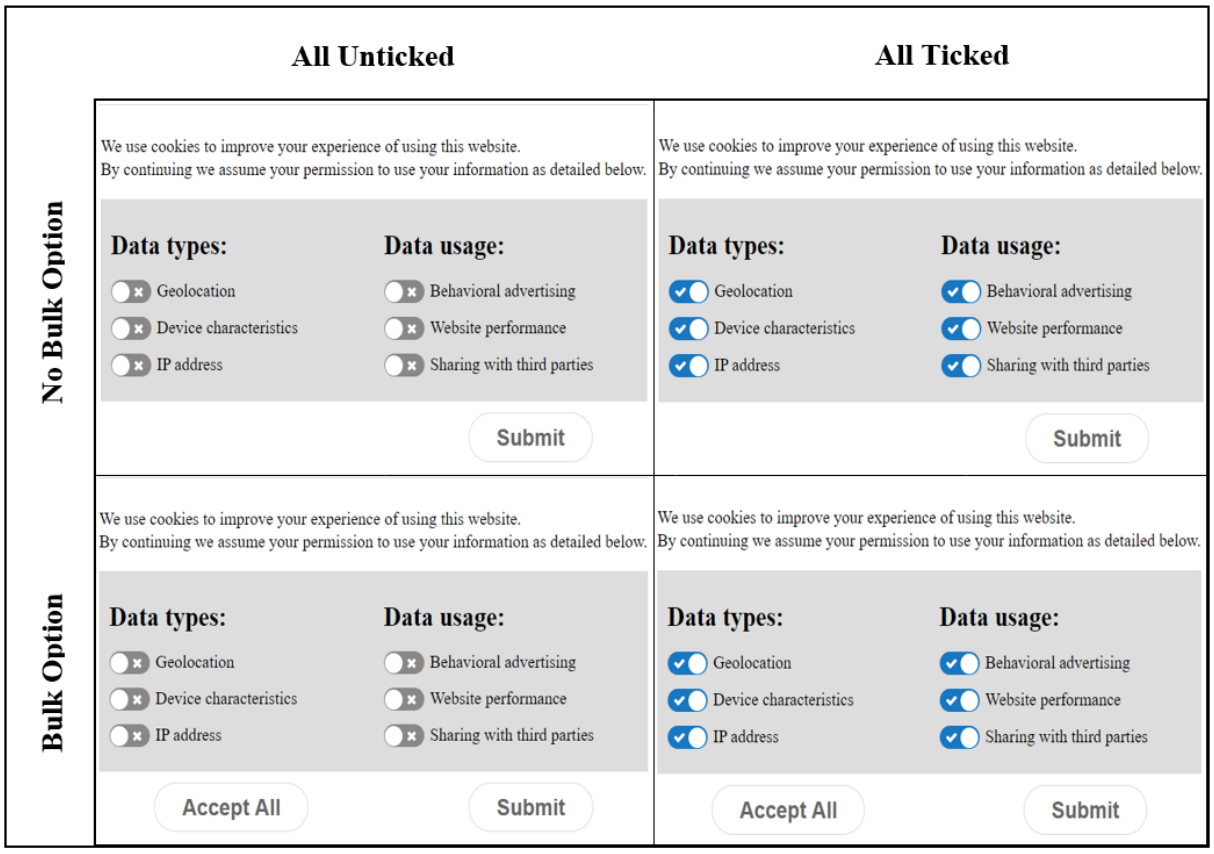
Samuelson, W. and Zechauser, R. 1988. 'Status Quo Bias in Decision Making'. *Journal of Risk and Uncertainty* 1 (1): 7–59.

Taylor, D. G., Davis, D. F. and Jillapalli, R. 2009. 'Privacy Concern and Online Personalization: The Moderating Effects of Information Control and Compensation'. *Electronic Commerce Research* 9 (3): 203–23.

Utz, C., Degeling, M., Fahl, S., Schaub, F. and Holz, T. 2019. '(Un)Informed Consent: Studying GDPR Consent Notices in the Field'. Proceedings of the 2019 ACM SIGSAC *Conference on Computer and Communications Security*, November, 973–90.

Appendix

Appendix A

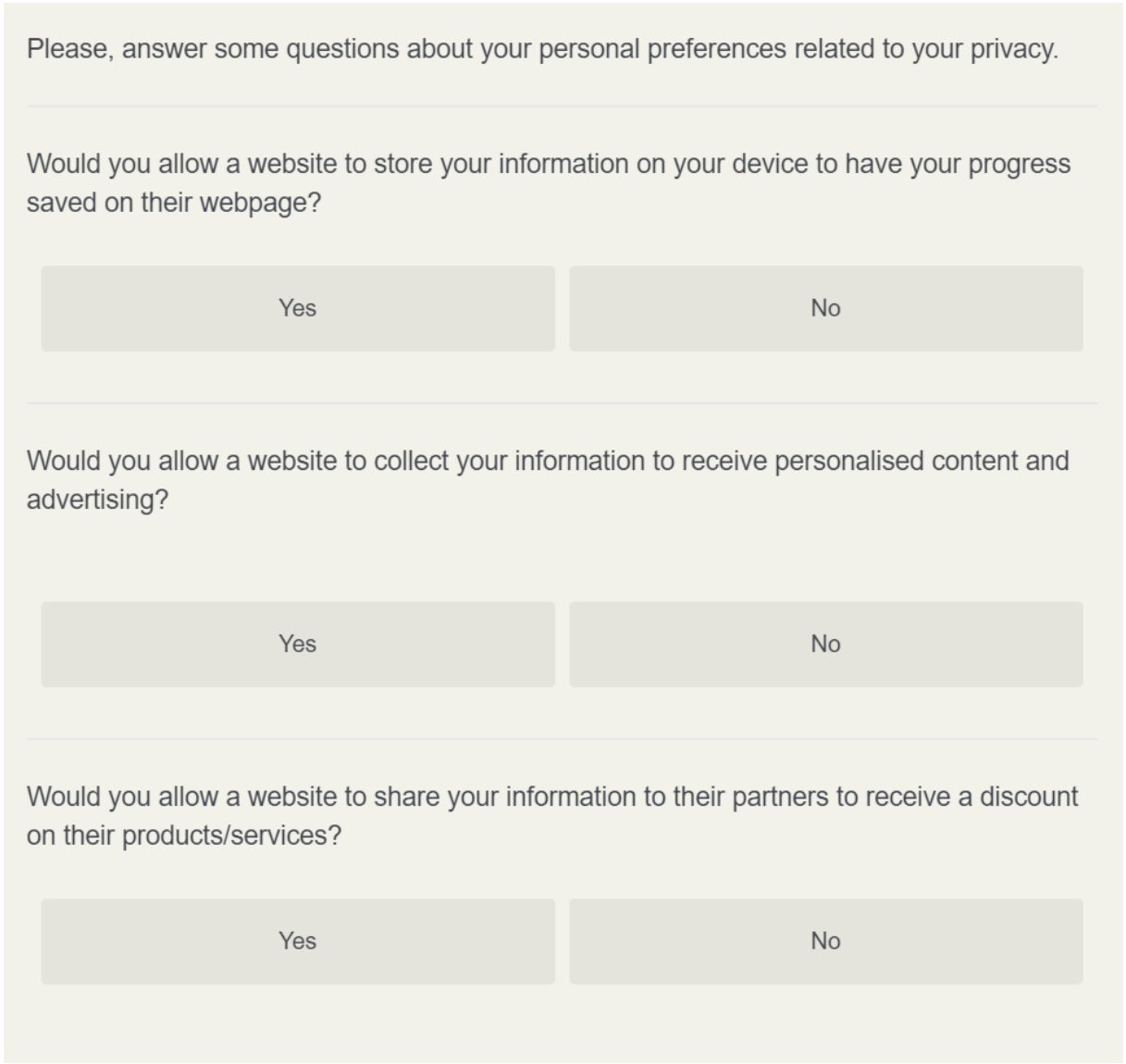


Appendix B

	Publishing permission Yes	Yes	No
Are you married?	☑	○	○
Have you ever been fired by your employer ?	☑	○	○
Have you ever stolen anything (e.g from a shop, a person)?	☑	○	○
Have you ever used drugs of any kind (e.g weed, cocaine, crack)?	☑	○	○
Have you ever lied about your age?	☑	○	○
Have you ever had cosmetic surgery?	☑	○	○
Have you ever done any kind of voluntary service?	☑	○	○
Have you ever had sex in a public venue (e.g restroom of a club, inside a car)?	☑	○	○
Have you ever made a donation to a non-profit organization?	☑	○	○
Do you have permanent tattoos	☑	○	○

Rating	Questions
Very intrusive	Q2: Have you ever been fired by your employer? Q3: Have you ever stolen anything (e.g.: from a shop, a person)? Q4: Have you ever used drugs of any kind (e.g.: weed, heroin, crack)? Q6: Have you ever had cosmetic surgery? Q8: Have you ever had sex in a public venue (e.g.: restroom of a club, airplane)?
Moderately intrusive	Q10: Do you have any permanent tattoos?
Not at all intrusive	Q1: Are you married? Q5: Have you ever lied about your age? Q7: Have you ever done any kind of voluntary service? Q9: Have you ever made a donation to a non-profit organization?

Appendix C


Please, answer some questions about your personal preferences related to your privacy.
Would you allow a website to store your information on your device to have your progress saved on their webpage?
Yes
No
Would you allow a website to collect your information to receive personalised content and advertising?
Yes
No
Would you allow a website to share your information to their partners to receive a discount on their products/services?
Yes
No

Appendix D

```r
within <- plm(p ~ ticked_banner + no_bulk_option + intrusive + ticked_survey + eu,
              data=dt.panel, index=c("id","q"), model="within")

random <- plm(p ~ ticked_banner + no_bulk_option + intrusive + ticked_survey + eu,
              data=dt.panel, index=c("id","q"), model="random")

phtest(within, random)
```

```
        Hausman Test

data:  p ~ ticked_banner + no_bulk_option + intrusive + ticked_survey +  ...
chisq = 8.1921e-14, df = 1, p-value = 1
alternative hypothesis: one model is inconsistent
```