DELab
DIGITAL RESEARCH STUDIES

WORKING PAPER #2/2021

WELFARE ASSESSMENT OF THE GDPR USING DISCRETE CHOICE EXPERIMENT

AUTHORS: MACIEJ SOBOLEWSKI[1,2], MICHAŁ PALIŃSKI[3]

[1] Joint Research Center, European Commission and University of Warsaw, Faculty of Economic Sciences. Corresponding author; email: maciej.sobolewski@uw.edu.pl

[2] This paper does not represent the point of view of the European Commission. The interpretations and opinions contained in this study are solely those of the authors.

[3] University of Warsaw, Digital Economy Lab & Faculty of Economic Sciences; email: m.palinski@uw.edu.pl

Citing: Sobolewski, M., Paliński, M., Welfare assessment of the GDPR using discrete choice experiment, DELab Digital Working Studies 2/2021, Warszawa 2021

Disclaimer: This is an updated version of the working paper Sobolewski, M., Paliński, M. (2017). How much consumers value on-line privacy?..., WNE Working Paper no. 17.

TABLE OF CONTENTS

ABSTRACT

Our paper analyses preferences towards new online mechanisms for protection of personal data mandated by the EU General Data Protection Regulation (GDPR). We estimate monetary valuation of the core instruments envisaged by the reform and assess potential welfare gains. On methodological grounds, we apply stated preference discrete choice experiment. With this approach, we provide *ex ante* insights into users' preferences towards particular privacy control mechanisms, such as right to be forgotten, right to object profiling and personal data portability. Our study is based on online survey of 143 Polish university students conducted before the GDPR implementation. We use these data to estimate mixed logit model. The main finding from the analysis is that introduction of the GDPR increases consumer surplus by improving control over sharing of personal data. The estimated value of median consumer surplus per capita amounts to 6.5 EUR per month. In the first place, users appreciate the right to be forgotten, extended information obligations and objection to profiling. Surprisingly, the role of personal data portability is sharply underestimated. Preference for the right to be forgotten is higher among more privacy concerned individuals and lower for those respondents who actively use larger number of online services. Intensive online activity increases demand for informative and user-friendly privacy policies.

Highlights

- We model preferences over personal data protection tools with a discrete choice experiment
- We estimate willingness-to-pay for specific protection mechanisms
- We estimate consumer surplus from the GDPR implementation
- We explore preference heterogeneity with users' attitudes towards privacy

Keywords

personal data management; online privacy; General Data Protection Regulation; mixed logit model; consumer surplus

JEL classification

C25; D12; L51

FUNDING

This research was supported by National Science Centre, Poland (grant number: 2017/25/N/HS4/01214).

INTRODUCTION

The GDPR has replaced legal basis for privacy protection in the EU adopted over 20 years ago when less than 1% of global population was using the Internet (WDI 2018). Not surprisingly, in times of user-generated information (Web 2.0) and data-driven economy this framework has lost adequacy. Therefore, the EU member states agreed upon the implementation of major reform regarding data protection framework. The rationale for the new regulation - General Data Protection Regulation (GDPR) was to enhance user privacy, which is understood as maintaining better control over sharing of personal information.

The GDPR extends the scope of informative obligations imposed on service providers and grants several control instruments to users, such as: (i) easier access to one's data, (ii) the right to be forgotten, (iii) objection to automated processing, (iv) portability of personal data and (v) objection to profiling (European Parliament 2016). Data portability, a particularly novel element of personal data protection regulation, might gradually shift the balance of power from online providers to end users. The term 'personal data' is broadly understood as any information relating to an identified or identifiable natural person. This functional definition includes not only traditional items like address or phone number, but possibly also wide range of new identifiers widely utilized in machine learning algorithms such as online activity data or shopping lists. The GDPR introduces two novel principles: privacy by design and privacy by default. Privacy by design requires that explicit consent to data processing for each specified purpose is required from the user. Moreover, personal data processing can be done only for purposes that are critical for operation of a service. Besides providers must set a maximal protection level as a default setting in their privacy policies.

Despite obvious benefits from sharing personal data online, behavioral studies document serious concerns related to potential abuse of such data (like hidden influence or manipulation) and insufficient protection of privacy. Both issues arise because of information asymmetry and incentives of data-intensive business models (Acquisti et al. 2015). On the other hand, it is well established

that declared privacy concerns often are not consistent with real behavior of users who do not read privacy policies or widely disclose personal data in social media. This ambivalent attitude, known as privacy paradox is a contextual phenomenon which has several causes, one of them being the lack of proper instruments to control the sharing of personal data on the Internet. If the GDPR is supposed to be an effective a policy response to this shortcoming, it has to be beneficial to Internet users to ensure wide adoption[1]. In the present study, we identify these benefits for particular instruments and *en block* for the whole package.

Our paper analyses the personal data protection reform in the EU from the perspective of user preferences. Our aim is to estimate monetary valuation of the core instruments envisaged in the GDPR and assess potential welfare gain from this policy intervention. Since our study uses data gathered before the GDPR implementation our evaluation has essentially *ex ante* character. On methodological grounds it utilizes stated preference discrete choice experiment as we have not yet observed any impacts of the GDPR on real behavior. Stated preference is a common approach in empirical research on privacy economics and previous empirical work focused mainly on estimating the value of personal data (Beresford et al. 2012; Carrascal et al. 2013; Potoglou et al. 2015). These valuations vary considerably because of a lack of efficient markets for personal data and associated common value benchmark. Our study focuses instead on privacy control mechanisms and provides estimates of welfare gain from policy intervention in privacy domain. By taking this perspective we fill a gap in literature and provide insights into users' preferences towards particular privacy control instruments, such as right to be forgotten, right to object profiling and personal data portability.

[1] Although the GDPR aims at harmonizing data protection law across the EU, there are areas in which the regulation leaves Member States space to adopt their own national rules.

This paper is organized in four main sections. In section I we briefly review literature on behavioral aspects of privacy and provide some evidence on users' attitudes towards privacy protection based on Eurostat data. In section II we describe our dataset. In section III we provide empirical assessment of welfare benefits from implementation of the main protection mechanisms envisaged by the GDPR and in section IV we explore preference heterogeneity.

I. LITERATURE REVIEW

The EC justifies the GDPR to a large extent with people's privacy concerns (European Commission 2017)[2]. But do Internet users really care about having control over personal information they share online? Surveys and polls show that online privacy is indeed an important concern for EU citizens. According to the results of the 2015 Eurobarometer's comprehensive survey more than eight out of ten respondents across EU feel that they do not have sufficient control over their personal data online (European Commission 2015). Among them two-thirds are concerned about that fact (Fig. 1, left pane). On the other hand, experimental studies indicate that individuals are willing to reveal their personal data, especially on social media (Acquisti et al. 2016). Also notwithstanding the stated concern and reluctance to share personal data online, Europeans often do not take basic actions preventing its unwilling disclosure such as: changing the privacy settings on social networks (Fig. 1, right pane). Such inconsistency between declared concerns and the actual behavior marks the ambivalence in the attitude towards privacy, known as 'privacy paradox' (Awad, Krishnan 2006; Holland 2009; Kokolakis 2017). The data from Fig. 1 supports the hypothesis about the existence of privacy paradox in the EU, particularly in central and southern member

[2] Other arguments pertain to the benefits for businesses stemming from harmonization of the legislatives of 28 member states.

states3. A possible explanation of the paradox is that privacy concerns have merely declarative character. Although this argumentation weakens the rationale for the GDPR reform, it is quite unlikely given a strong empirical evidence showing that users substantially value their personal data4. More plausible explanations refer to the other side of the paradox, pointing to lack of risk awareness from information disclosure or lack of skills and tools to protect personal data. Privacy paradox can also be reconciled with so called privacy calculus argument which states that in certain situations the benefits from information disclosure can outweigh potential damages. Certainly, strengthening the users' control over their personal information helps to protect personal data in certain contexts while allowing for benefits from sharing it in other situations.

The economics of privacy starts with the observation that 'personal data have been commodified into a tradeable asset' (Preibusch 2015). Research body in privacy economics is growing fast since early 2000s, following rapid development of the Internet and proliferation of business models based on intensive processing of personal data acquired via online interactions (Acquisti et al. 2016). The two main streams of empirical work focus on determination of monetary value of personal data and on valuation of selected control functionalities, mainly protection from unauthorized secondary use of data. With respect to information valuation two general methodological approaches might be distinguished, based on either market valuation or individual perception of personal data value (OECD 2013). The latter approach is more frequently adopted because instead of relying on rarely accessible actual data, it utilizes various types of economic experiments. Laboratory and field experiments on the one hand measure the value consumers attribute to per-

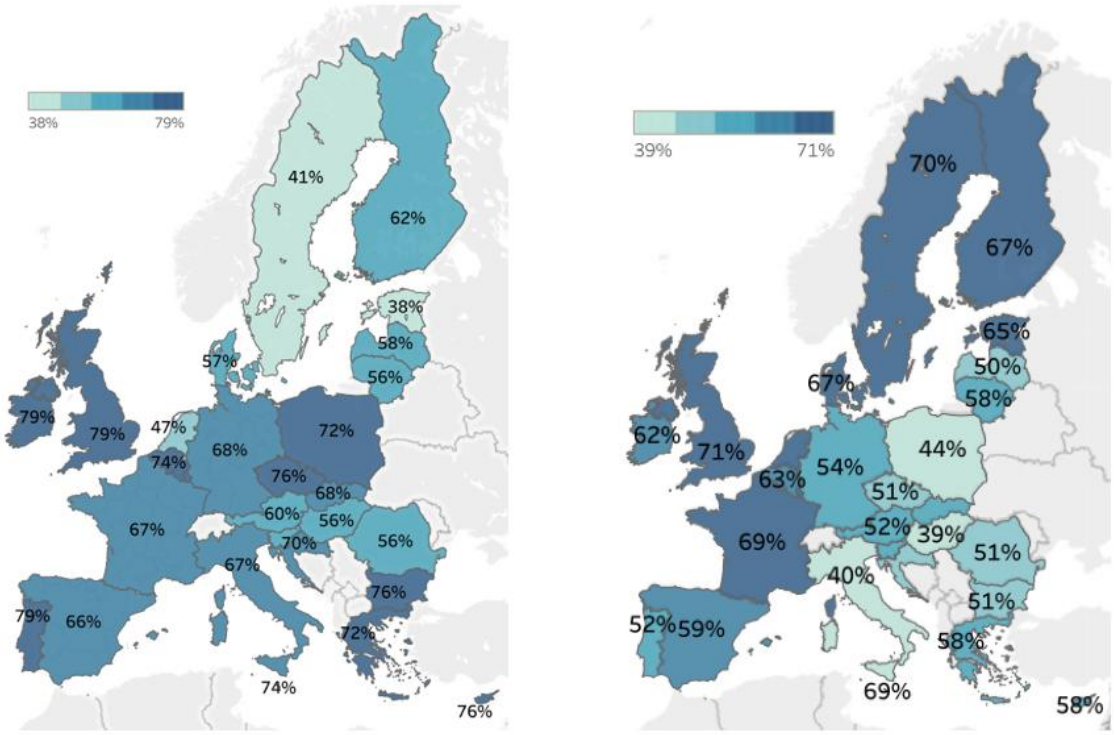
[3] The choropleth map shows that in these regions we observe a combination of high percentage of respondents concerned about not having complete control over the information provided online and relatively low percentage of respondents who have tried to change the default privacy settings on social networks.

[4] For a review of studies examining the users valuation of personal data see: Table 1.

sonal data based on actual purchase transactions. Revealed preference data can also be used to examine a trade-off between privacy control and remuneration. On the other hand, discrete choice experiments (DCE) focus on catching the same trade-off through survey-based hypothetical settings. The main advantages of DCE over field experiments result from greater flexibility and variability of data and ability to capture the value of enhanced privacy tool in the specific context for which revealed preference data is not available or non-existent (as is the case of the GDPR).

In the Table 1 we provide the summary of the main empirical studies which derive valuations for privacy and personal data: willingness-to-pay (WTP) for enhanced protection and willingness-to-accept (WTA) for disclosure of different types of personal information. The majority of both WTP studies focus on assessment of single privacy enhancing mechanism. Among WTP studies the main strand of research deals with monetary value estimation of protection from the unwilling secondary use of personal data and its disclosure to the third parties. There are several studies dealing with privacy management issues: personal data storage and portability, refrain from personalized advertisement, protection from telemarketing. WTA research examines valuation of geolocation and transaction data. Recently few studies examined the gap between WTA and WTP for personal data and tend to associate it with the endowment effect (Acquisti et al. 2013).

Fig.1. A glance on privacy paradox across EU.



Left pane (N=16244): Concern about not having complete control over the information provided online (among respondents who feel that they do not have complete control over their personal data online). Right pane (N=15339): Respondents who have tried to change the privacy settings of personal profile from the default settings on social networks (base: respondents who use online social networks).

Source: Own elaboration based on data from Eurobarometer 431/Wave EB83.1 (European Commission 2015).

Table 1. Studies measuring valuations of online personal data.

(A) Willingness-to-pay (WTP) for protecting personal data.

Country	Study	Type of study	Preferences	Object of valuation	Main results
EU 27	Patil et al. (2015)	DCE	Stated preferences	Privacy enhancing services	WTP a monthly premium for privacy enhancing services (ISP hides information on users' online activity and warns user which

					websites do not meet desired level of privacy): in the lowest income group about 3EUR; in the highest income group about 5EUR. Younger people (18–24) are less willing to pay for avoiding tracking of their online activity, older people (65+) are more willing to pay for privacy enhancing services.
UK	Potoglou et al. (2015)	DCE	Stated preferences	Protection from secondary use of personal data	WTP to avoid sharing personal data (PD) with third parties: 5.57GBP per transaction; value of shortening the period PD is stored by a retailer from 5 to 1 year: 2.68GBP. Value of a free service is not enough to compensate for disutility generated by secondary use of customer information.
US	Butler and Garrett (2014)	DCE	Stated preferences	Protection from secondary use of personal data	WTP for not sharing video streaming usage information with third parties: 4USD per month; for not sharing both usage and personal identity information: 6USD per month.
US	Egelman et al. (2013)	Field experiment	Stated preferences	Privacy enhancing application	WTP for an application requesting the least amount of PD: 1.5USD among privacy-conscious participants (25%); 80% of the participants were not willing to pay more than 0.99USD for a version of the app that does not collect the PD for targeted advertisement.
DE, AT	Bauer et al. (2012)	Field experiment	Stated preferences	Facebook data portability	Almost half of participants were not willing to pay for storing their FB content and transferring it to another platform (Google+), average one-time WTP: 9.5USD,

					maximum WTP: 150USD.
US	Tsai et al. (2011)	Lab experiment	Revealed preferences	Intuitive formulation of privacy policy	WTP a premium for product provided with intuitive privacy policy written in plain language: 0.6USD (about 4% of the price of the product in question).
FR, DE, UK, RU	Krasnova et al. (2009)	DCE	Stated preferences	Refrain from personalized advertising	Average WTP for avoidance of personalized advertising by online social network using user's demographic information: 14-17EUR per year. Privacy concerned users are willing-to-pay between 23-28EUR annually for the same service.
US	Png (2007)	Market valuation	Stated preferences	Protection from telemarketing	WTP for avoiding telemarketing by signing in to the federal 'do not call registry': between 13.2 and 98.3USD annually.
US	Hann et al. (2007)	DCE	Stated preferences	Protection from secondary use of personal data	WTP for protection from improper access, and secondary use of personal information range between 30 and 45 USD.
US	Varian et al. (2005)	Market valuation	Stated preferences	Protection from telemarketing	Value of federal 'do not call' registry varies from 0.6USD to 33USD per household per year.
US	Hann et al. (2002)	DCE	Stated preferences	Protection from secondary use of personal data	WTP for disagreement to secondary use of personal information is worth between 40 and 50USD. The cost-benefit privacy trade-offs are not related to personal characteristics such as gender, contextual knowledge or general trust.

(B) Willingness-to-accept remuneration for disclosing personal data.

Country	Study	Type of study	Preferences	Object of valuation	Main results
ES	Carrascal et al. (2013)	Field experiment (reverse second price auction)	Stated preferences	Disclosure of offline vs online identity	Users value their 'offline' identity more than the 'online' one. Median WTA disclosure of information about age and address: 25EUR, median WTA share online browsing history: 7EUR.
DE	Beresford et al. (2012)	Field experiment	Revealed preferences	Disclosure of e-commerce transaction	WTA 1EUR discount for providing date of birth and monthly income.
BE, CZ, DE, GR, SK	Cvrcek et al. (2006)	Field experiment (reverse second price auction)	Stated preferences	Disclosure of location data to third parties	WTA disclosure of location data acquired by mobile application: 43 EUR monthly.
UK	Danezis et al. (2005)	Field experiment (reverse second price auction)	Revealed preferences	Disclosure of location data to third parties	Median WTA disclosure of location data acquired by mobile application: 10GBP monthly. The WTA of respondents travelling more intensively rose significantly.

Evidence from the studies listed in Table 1-A suggests that the willingness-to-pay for protecting personal data is rather noticeable. Likewise, people tend to ask for high compensations for disclosing their data to providers (see the studies listed in Table 1-B). As already noted WTA valuations seem to exceed commercial value as a result of private signal bias. On the other hand, experimental WTP measures can suffer from insufficient incentive compatibility of treatment. In discrete choice experiments this problem can be addressed indirectly by establishing consequentiality between the choices and resulting regulation (Carson, Groves, List 2014).

Our study contributes to the first strand of literature (Table 1-A). Instead of a single instrument or functionality, our study focuses on a valuation of the whole set of protection and control instruments enhancing individual privacy online.

If the personal data is a valuable asset for the end-user as several empirical studies suggest, it is rational to assume that implementation of enhanced control mechanisms over this asset will generate positive welfare effects. We estimate the change in consumer surplus resulting from implementation of the GDPR using data from stated-preference discrete choice experiment study. Based on hypothetical choices reported by a sample of N=143 individuals, we elicit users' preferences over privacy protection policies and calculate willingness to pay for particular protection mechanisms: right to be forgotten, portability of data, extended informative obligations and right to object profiling. Based on WTP distributions for each mechanism, we then calculate the gross monetary gain across the whole sample of users from adoption of particular (mandatory) combination of protection instruments as envisaged by the GDPR.

II. DATA

The data was collected in the internet survey in 2017. Final sample used in the study is composed of 143 students from various faculties of University of Warsaw in Poland. For that reason our results cannot be treated as representative to the any wider population, however they might reflect a preference of the most active group of young internet users, who usually have several accounts on different online platforms. The average number of online accounts exceeds six, with Facebook and Skype being the two most popular services (see Table 2 for sample characteristics). Examining the preferences of digital natives towards protection of personal data is particularly meaningful. This group faces privacy related trade-offs on everyday basis and undoubtedly will be affected by the new privacy regulation. This adds up to the consequentiality of their declared choices and increases reliability of collected data and results. Participants' ages ranged from 18 to 48 years old (mean = 21) and 60% of them are female. Almost 40% of the participants work part time; the me-

dian of the reported net individual monthly income is between 360 and 480 Euro (net minimum wage in Poland in 2017 was ~360 EUR per month). Table 2. Sample characteristics.

Variable	**Sample**
Gender (female)	60%
Age	Mean = 21 SD = 3.7
Monthly net income	Median: 1501-2000 PLN (~360-480 EUR)
Online platforms and communication apps accounts and activity	Mean = 6.6 (out of 8) Top two: Facebook: 95% Skype: 76% Last two: Pinterest: 13% Twitter: 20%
Have you ever resigned from registration to an online service because of its privacy policy?	Yes: 65%

Each respondent was presented with ten choice tasks, each having 3 policy options: two hypothetical and the current scope of protection (status quo). Hypothetical options varied with respect to the availability of particular protection mechanisms and also their scopes. The number of attributes and their levels was too large for implementation of the full factorial plan. In this study, we applied an efficient experimental design. This approach minimizes standard errors of the utility parameters based on some prior information about parameter values (Sándor and Wedel 2001).5 It has been shown that efficient plans extract more information from respondent choices than orthogonal plans (Street and Burgess 2007). In our study, experimental plan was optimized with respect to D-Error. The list of attributes and their levels as well as example of the choice card are presented in Appendix (see Tables A1, A2).

Hypothetical character of stated choice and lack of true budget constraint are pointed among main disadvantages of this approach potentially leading to hypothetical bias (Ben-Akiva et al. 1994; Train 2009). Nevertheless, properly designed discrete choice experiments can mitigate those concerns. Numerous evidence from discrete choice models on stated and revealed preferences points to lack of statistical differences between estimates from models on the two types of data (Carson et al. 1996; Whitehead et al. 2010). Moreover, in our case the use of stated preference data was the only possible choice because we study preference over future policy intervention, hence no actual data exists yet.

[5] We obtained priors from declared reservation prices collected in the pilot phase of the survey.

III. ECONOMETRIC FRAMEWORK

Formally, discrete choice modeling is based on the random utility model (McFadden 1974). In this framework, the utility function of consumer $i \in I$ from alternative $j \in J$ in choice situation $t \in T$ can be expressed as:

$$U_{ijt} = \boldsymbol{\beta}' \boldsymbol{x}_{ijt} + \varepsilon_{ijt} \qquad (1)$$

where $\boldsymbol{\beta}$ is the vector of utility parameters, $\boldsymbol{x}$ is the vector of observed attributes specific to the consumer the alternative j and choice situation t, and ε is the random component, representing the joint influence of all unobserved factors that influence decision-making. By assuming that the random component is identically and independently Gumbel distributed, the multinomial logit (MNL) model is obtained which has a familiar, closed-form expression for the choice probabilities of each alternative (Greene 2011). In this study, we apply a mixed logit (MXL) extension to take the respondents' preference heterogeneity into account (Greene and Hensher 2007). MXL model treats that consumer *i* has specified, albeit non-observable, parameters of the utility function which follow a priori specified distributions in a population $\boldsymbol{\beta}_i \sim f(\boldsymbol{b}, \boldsymbol{\Sigma})$, where $\boldsymbol{b}$ is the vector of the mean values of parameters and $\boldsymbol{\Sigma}$ is their variance-covariance matrix (possibly non-diagonal to account for correlations across alternatives or choice situations). By assuming a structured variation of individual tastes in the sample, in the form of individual-based parameters, the MXL model is more realistic and typically yields a much better fit to the data. This benefit comes at the cost of a more complicated estimation procedure. In a discrete choice experiment, P_{ijt} – the unconditional mixed logit probability of choosing alternative j in situation t by consumer i - is an integral of standard logit probabilities over a density individual utility parameters. Since mixed logit probabilities involve integrals which do not have closed forms, unconditional probabilities must be simulated by taking multiple random draws from respective joint distribution and averaging (Train 2009). In the final step, the sequence of T choices made by each person during the experiment are

represented by the log-likelihood function from which estimators of $\boldsymbol{b}, \boldsymbol{\Sigma}$ can be obtained numerically from maximization of the following log-likelihood function:

$$LL = \sum_{i=1}^{I} log \frac{1}{D} \sum_{d=1}^{D} \prod_{t=1}^{T} \sum_{j=1}^{J} y_{ijt} \frac{exp\,(\boldsymbol{x}_{ijt}\boldsymbol{\beta}_i)}{\sum_{j=1}^{J} exp\,(\boldsymbol{x}_{ijt}\boldsymbol{\beta}_i)} \quad (2)$$

where y_{it} is a dummy variable equal to 1 if respondent *i* selected alternative *j* in choice situation *t* and 0 otherwise and *D* represents the number of draws taken from joint normal distribution.6 With linear utility function, a consumer's willingness-to-pay for a change in an attribute $k \in K$ is defined as the ratio between the parameter of interest and the minus price attribute, as income is usually missing (Bliemer and Rose 2013):

$$WTP_k = -\frac{ß_k}{ß_{price}} \quad (3)$$

This is equivalent to calculating a marginal rate substitution between attribute *k* and monetary variable. In MNL model, both coefficients are fixed, but uncertain due to a sampling variance. Hence, WTP given in Eq. (3) is, in fact, a random variable, for which point estimate calculated from MNL coefficients might have distribution with undefined moments. To overcome this problem WTP measure and corresponding confidence intervals are calculated from a simulation (Krinsky and Robb 1986). In MXL, the simulation of WTP is more complicated as both coefficients are random variables following specific distributions assumed by the modeler. In this study we use an extended two-step version of Krinsky and Robb method in which instead of fixed coefficients, individual parameters from their assumed distributions are drawn in a simulation (Hensher and Greene 2003; Bliemer and Rose 2013). In this way we obtain full distributions of WTP which is useful for calculation of consumer surplus. Since the scope of new regulation is already known we

[6] The mixed logit model was estimated using R with 300 Halton draws.

derive simulated change in consumer surplus from introduction of the GDPR by summing individual WTP measures for a combination of attributes which reflect new policy and subtracting the sum of WTP for the current policy (status quo alternative).

IV. RESULTS

Our final dataset consisted of 4390 choices made by 143 respondents. We used these data to estimate the mixed logit model, assuming that all of the preference parameters for various protection mechanisms were random, following normal distributions and lognormal distribution (for minus the cost coefficient). We assumed the following form of the utility function of respondent $i \in I$ from choosing alternative $j \in J$ in choice situation $t \in T$ (time subscript is suppressed):

$$U_{ij} = \beta_{1i} INFDUTY\_E_{ij} + \beta_{2i} INFDUTY\_R_{ij} + \beta_{3i} INFDUTY\_SQ_{ij} + \beta_{4i} PROFILING_{ij} + \beta_{5i} FORGET\_E_{ij} + \beta_{6i} FORGET\_R_{ij} + \beta_{7i} FORGET\_SQ_{ij} + \beta_{8i} INTERFACE_{ij} + \beta_{9i} PORTABILITY_{ij} + \beta_{10i} COST_{ij} + \epsilon_{ij} \quad (4)$$

where $\boldsymbol{\beta}$ is the vector of parameters associated with their respective variables and ε_{ij} is a random component of utility associated with alternative j. The interpretation of variables in the choice model is given in Annex (see Table A1). The estimation results – coefficients for means and standard deviations of the normally distributed preference parameters for MXL – are reported in Table 3 below. We set FORGET_SQ and INFDUTY_SQ as the baseline categories so that estimated parameters describe the importance (utility) associated with the attribute levels relative to current status quo. Their absolute values do not have an interpretation, but their sign, relative values, and statistical significance indicate the most important mechanisms to which the respondents pay the greatest attention.

Table 3. The results of the MXL model of respondents' choices over different privacy protection policies.

Variables	**Parameters**	
(see Table A1 in Annex for more detailed definitions)	**Mean**	**Standard deviation**

	(s.e.)	(s.e.)
INFDUTY_E - extended scope of information duty relative to SQ (n)	0.880***	1.016***
	(0.156)	(0.217)
INFDUTY_R – reduced scope of information duty relative to SQ (n)	-1.006***	1.201***
	(0.2326)	(0.273)
PROFILING – right to object profiling (n)	0.865***	1.139***
	(0.147)	(0.214)
PORTABILITY – right to port personal data (n)	-0.197	0.934***
	(0.135)	(0.204)
FORGET_E – extended right to be forgotten compared to SQ (n)	1.267***	0.997***
	(0.168)	(0.234)
FORGET_R – reduced right to be forgotten relative to SQ (n)	-1.026***	1.088***
	(0.197)	(0.255)
INTERFACE – integrated privacy management (n)	0.381***	0.832***
	(0.135)	(0.228)
(minus) COST – monthly fee (ln)	-1.778***	1.494***
	(0.116)	(0.146)
Model characteristics		
Log-likelihood	-1,038.106	
McFadden's pseudo R2	0.339	
n (observations)	143(4290)	
k (parameters)	16	

***, **, * Significance at 1%, 5%, 10% level; (n) – normal distribution; (ln) lognormal; SQ – status quo/current policy.

For example, positive coefficients for extended scope of information duty (*INFDUTY_E*), right to object profiling (*PROFILING*) or right to be forgotten (*FORGET_E)* indicate that presence of these mechanisms increase the value of proposed policy. Large and significant standard deviations indicate a considerable individual heterogeneity of preferences in the sample. Except of portability, all the coefficients for means have expected signs and are statistically significant. In case of personal data portability the average impact is close to zero, however significant coefficient for standard deviation reflects the presence of individuals with opposing (positive and negative) perceptions of this mechanism. This is the most striking results of our analysis which indicates, that users do not recognize the importance of data portability in the new regulation. Most probably lack of appreciation results from lack of experience with this mechanism and consequently lack of awareness of the benefits it might potentially bring. We have also tested to what extent users are keen on using integrated solution for management of their personal data (*INTERFACE)*. In principle, thanks to data portability, the GDPR would allow for a one-stop-shop management of all online accounts, including porting data between providers and data erasure. Integrated solution would open floor for totally new services based on data brokerage. Interestingly, coefficient for such an interface occurred to be only moderately positive compared to main privacy control mechanisms. This indicates that more advanced solutions for data management are premature at the current level of user awareness.

Estimated coefficients of utility function, allow for determination on what terms respondents are willing to trade one attribute for another. This information can be presented in money metric terms through willingness to pay. This measure informs about the rate at which respondents are

willing to exchange their money for the change in particular attribute level. In Table 4 we present median WTP estimates in our sample, based on coefficients from MXL model[7].

Table 4. Willingness to pay for privacy policy characteristics [PLN][8].

Variables	Median WTP (s.e.)	95% c.i.
1. INFDUTY_E - extended scope of information duty relative to SQ	3.45 (1.03)	1.86 – 5.95
2. INFDUTY_R – reduced scope of information duty relative to SQ	-3.67 (1.13)	-6.14 – -1.82
3. PROFILING – right to object profiling	3.23 (0.86)	1.83 – 5.24
4. PORTABILITY – right to port personal data	-0.45 (0.44)	-1.61 – 0.20
5. FORGET_E – extended right to be forgotten compared to SQ	5.72 (1.19)	3.75 – 8.31
6. FORGET_R – reduced right to be forgotten relative to SQ	-3.88 (1.12)	-6.48 – -2.11
7. INTERFACE – integrated privacy management	1.22 (0.55)	0.27 – 2.47

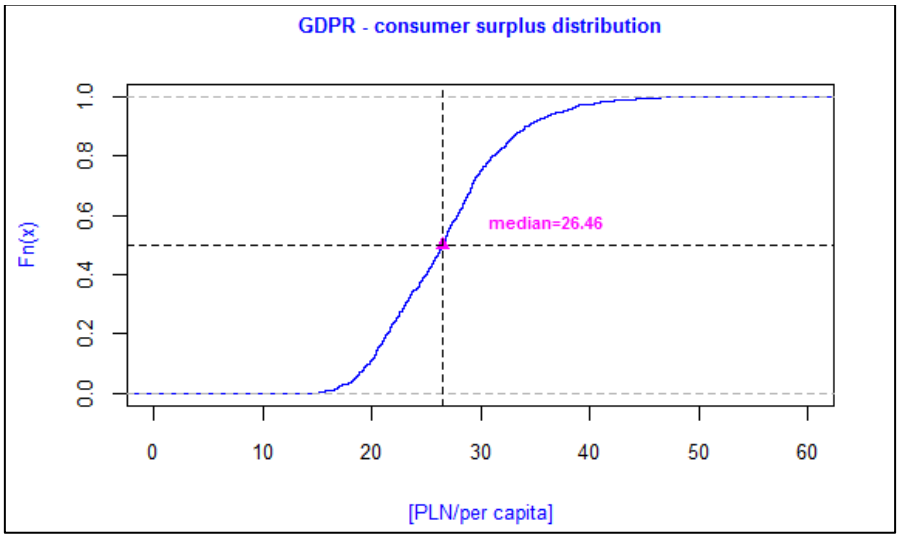
[7] WTP estimates have been obtained using two stage Krinsky and Robb simulation with 10^3 random draws at each stage. In the first stage we draw a vector of means and standard deviations of the utility parameter distributions. In the second stage, for each realization we draw a sample of individual utility parameters.

[8] 1 PLN ≈ 0.25 EUR

	Gross consumer surplus per capita (s.e.)	95% c.i.
implementation of the GDPR package (attributes 1, 3, 4, 5)	26.14 (6.17)	16.88 – 39.98

Calculated WTP measures indicate that respondents assign substantial monetary value to particular mechanisms. For example, the right to erasure of personal data is worth an additional 1.4 EUR (5.72 PLN) per month for. Extended information obligation for online providers and right to object profiling are both valued similarly, at around 0.80 EUR each. Implicit prices for reduced levels of information obligation (*INFDUTY_R)* and right to be forgotten (*FORGET_R)* are negative and showing the monetary magnitude a loss from assumptive suspension of information duties or abolition of right to erase personal data compared to their status quo levels. Finally, we have derived the surplus gain from the combination of attributes that together make up for the scope of the GDPR. This combination assumes extended information duty, right to object profiling, right to port personal data and extended right to be forgotten. The gross consumer surplus is calculated as the sum of willingness to pay for the implementation of 'the GDPR policy alternative' in the entire sample. Since our WTP measures come from simulation, we obtain a whole distribution of gross consumer surplus (see Fig. 2). Its median value amounts to 6.5 EUR monthly (26 PLN) in per capita terms. We consider this level as substantial, given that the monthly price for broadband access in Poland is around 10-12 EUR. Importantly, our result is not yet another valuation of personal data. The benefits from the GDPR stem from reduction of asymmetry and gaining control over personal data. Importantly, people may still decide to disclose specific data for free to gain more accurate search results or other benefits. However, with the GDPR they can better protect those data which they do not want to share.

Fig. 2. Distribution of simulated consumer surplus from implementation of the GDPR.



Source: Own elaboration.

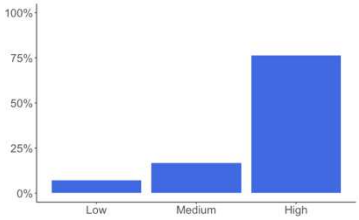
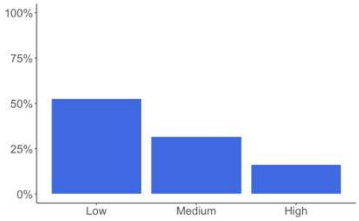
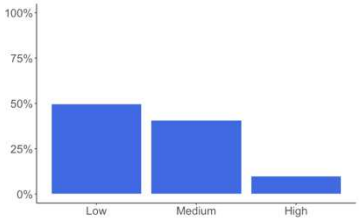
V. PREFERENCE HETEROGENEITY

As part of the survey, respondents were asked to declare their online activity and indicate their preferences towards a series of statements regarding online privacy awareness, attitudes and practices. The aim of these questions was to construct three attitudinal and behavioral indices with which we classify our respondents. We used those indices to explain considerable preference heterogeneity observed in our sample, as indicated by large and statistically significant estimates of standard deviations of parameter distributions shown in Table 3.

Two indices: Privacy Concern Index (PCI) and Privacy Protection Awareness Index (PPAI) correspond to psychometric scales validated in previous studies (Potoglou et al. 2015; Buchanan et al. 2007). PCI measures concern about uncontrolled usage of online personal data by service providers and third parties. PPAI tracks respondents' knowledge about online privacy mechanisms and basic steps taken by them to control digital footprints. Finally, we designed the Online Activity Index (OAI) to capture the respondents' presence and activity on online platforms and usage intensity of popular online services. For the in-sample distribution of indices see Table 5. Details re-

garding the construction of each index along with mean results for the individual questions are provided in Appendix (see Tables A3 and A4).

Table 5. Indices built to explore preference heterogeneity.

Index	Description	Results
Privacy Concern Index (PCI)	Measures concern about uncontrolled usage of online personal data by service providers and third parties	
Privacy Protection Awareness Index (PPAI)	Assesses knowledge about online privacy mechanisms and steps taken to control digital footprints	
Online Activity Index (OAI)	Measures presence and activity on online platforms and usage of online services	

Histograms presented in Table 5 indicate that over 75% of individuals in the sample are highly concerned about their online privacy. With regards to protection awareness our sample is more differentiated. Nearly half of respondents poses at least medium awareness about privacy protection measures, including basic ones such as privacy policy settings and more advanced tools such as use of VPN for anonymity. On the other hand, the remaining 52% of the respondents have the lowest score on the awareness scale. This is worrisome, given that we have surveyed mostly well-educated digital natives. Online activity score combines the number of online services with the frequency of their use. Our respondents are present on several online platforms but with one ex-

ception (Facebook) they do not use them on the daily basis. Interestingly, online activity index is moderately positively correlated with protection awareness and privacy concern, but the latter two indices are independent in the whole sample (see Table 6). Users who spend much time online are more likely to be exposed to the privacy management issues and at the same time are likely to become more concerned about their control over personal data online.

Table 6. Spearman correlations between indices.

	OAI	PPAI	PCI
OAI	1		
PPAI	.31***	1	
PCI	.15***	.02	1

***, ** Significance at 0.1%, 1%

Altogether we expect that privacy concern index should explain heterogeneity of preferences towards most tangible protection mechanism, such as right to be forgotten or objection against profiling. Also, individuals with higher scores of online activity index should appreciate more the GDPR provisions. We test those hypotheses by allowing the distributions of random parameters to be heterogeneous with observed respondent characteristics ($\boldsymbol{z}_i$). Formally, $\boldsymbol{\beta}_i \sim f(\boldsymbol{b} + \boldsymbol{\Delta z}_i, \boldsymbol{\Sigma} + \boldsymbol{\Gamma z}_i)$, where $\boldsymbol{\Delta}$ and $\boldsymbol{\Gamma}$ are estimable vectors of parameters that enter heterogeneous means and variances of random parameters. In what follows we explore individual heterogeneity in means with a vector of three indices: $\boldsymbol{z}_i = \{PCI_i, PPAI_i, OAI_i\}$. We consider all extended attributes denoting enhanced protection options: *INFDUTY_E, PROFILING, PORTABILITY, FORGET_E, INTERFACE.* More specifically, parameter $\beta_{PORTABILITY\_i}$ has now the following distribution:

$$\beta_{PORTABILITY_i} \sim N\left(b_{PORTABILITY} + \Delta_{PCI\,PORTABILITY} PCI_i + \Delta_{PPAI\,PORTABILITY} PPAI_i + \Delta_{OAI\,PORTABILITY} OAI_i, \sigma^2_{PORTABILITY}\right) \quad (5)$$

Similar expressions to Eq. 5 are introduced for the remaining enhanced protection options. The results of this model are reported in Table 7. Explaining heterogeneity with covariates slightly improves model performance as indicated by an increase in the pseudo-R2 in comparison to the baseline model. The coefficients given in panel A should be interpreted together with the coefficients in panel B. In what follows we concentrate solely on the marginal effect of covariates on the means of normally distributed random parameters presented in panel B.

Table 7. The results of MXL model with covariates of means of normally distributed random parameters.

	A. **Parameters of MXL**	
	Mean (s.e.)	**Standard deviation (s.e.)**
INFDUTY_E - extended scope of information duty relative to SQ (n)	-0.001 (1.062)	1.256*** (0.329)
INFDUTY_R – reduced scope of information duty relative to SQ (n)	- 1.142*** (0.279)	1.400*** (0.329)
PROFILING – right to object profiling (n)	- 0.107 (1.052)	1.159*** (0.232.08)
PORTABILITY – right to port personal data (n)	0.085 (0.904)	0.738*** (0.237)
FORGET_E – extended right to be forgotten compared to SQ (n)	- 1.075 (1.271)	1.052*** (0.261)
FORGET_R – reduced right to be forgotten relative to SQ (n)	- 0.999*** (0.232)	1.099*** (0.248)
INTERFACE – integrated privacy management (n)	1.044 (0.960)	1.008*** (0. 253)
(minus) COST – monthly fee (ln)	- 1.952*** (0.170)	1.323*** (0.185)

B. Coefficients (with s.e.) of covariates of means of random parameters

Covariates	**INFDUTY_E**	**PROFILING**	**PORTABILITY**	**FORGET_E**	**INTERFACE**
PCI – privacy concern index	0.068 (0.347)	0.472 (0.387)	0.342 (0.305)	1.176** (0.460)	- 0.536 (0.341)
PPAI – privacy protection awareness index	- 0.239 (0.265)	0.281 (0.276)	- 0.517*** (0.224)	0.468* (0.270)	0.147 (0.253)

OAI – online activity index	0.680** (0.322)	- 0.385 (0.268)	0.072 (0.229)	- 0.966*** (0.289)	0.352 (0.324)
C. Model characteristics					
Log-likelihood	-1017.14				
McFadden's pseudo R2	0.352				
n (observations)	143 (4290)				
k (parameters)	31				

***, **, * Significance at 1%, 5%, 10% level

The chosen covariates partially explain unobserved preference heterogeneity in our sample. Primarily, we observe that stronger preferences for the extended right to be forgotten occur among individuals who voice stronger concerns about their online privacy (increasing values of PCI correspond to greater utility from FORGET_E). Furthermore, we observe that individuals who declare more intense online activity (OAI) have greater utility from extended scope and friendlier form of privacy policies (INFDUTY_E). On the other hand, this segment of users appreciates much less than others the right to be forgotten as indicated by negative utility coefficient for FORGET_E (-0.966). It might be explained by the alleged higher level transparency and openness among individuals active on several online platforms. Those results are in line with our expectations. Interestingly a high level of e-privacy awareness (PPAI) reduces the utility from personal data portability. This is an unexpected result. We would anticipate that individuals acquainted with e-privacy control tools would rather be gaining utility from being able to easily transfer their personal data among online services providers. We consider the obtained result as a manifestation of a lack of confidence of privacy conscious users in service providers to port their personal. Nevertheless, this result shows a demand for social advertising to raise awareness of portability.

CONCLUSION

In 2010 Facebook aroused controversy by introducing new default privacy settings for its 350m users[9]. According to numerous civil liberties campaigners as well as some consumer protection organizations the change was clearly intended to push the platform's users to expose more personal data online while decreasing their control over shared information (Bankston 2009)[10]. However, Mark Zuckerberg CEO of Facebook justified the privacy deregulation at that time by claiming that: "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time" (Johnson 2010). So is privacy in the digital era indeed a thing of the past? Exponential growth of online platforms fueled by utilization of personal data, development of predictive analytics for re-identification of anonymous individuals or last but not least the Snowden affair all suggest in favor of that statement (Crawford and Schultz 2014; Dix et al. 2013). But, even if we agree that disclosing personal information is an increasing part of modern life, Internet users still signal concerns about control of online privacy. To what extent these concerns could be mitigated by new regulation on data protection? This study addressed this question by providing an insight into preferences towards online privacy of a group of digital natives from Poland.

The main finding from the analysis is that implementation of enhanced privacy control mechanisms generates positive welfare effect. The size of estimated welfare gain from policy intervention of the same scope as the GDPR amounts to 6.5 EUR per capita monthly. This result proves that there is a 'demand' for privacy reform driven by both concerns related to disclosing personal

9 In the Q1 2017 Facebook had already 1.9 bln active users.

[10] The privacy setting change gave the users chance to alter settings on items they upload to the site, such as photographs and videos, but all of their status updates were automatically made public unless specified otherwise.

data as well as shortage of effective tools for privacy management. The benefits from the GDPR stem from reduction of asymmetry and gaining greater control over sharing of personal data. Importantly people may still want to disclose their data for free to gain more accurate search results or other benefits, however with the GDPR they are able to control in a better way various types of information which they are not willing to disclose. In this sense the GDPR can become a catalyst of end-user oriented personal data markets and we are not surprised that it provides value added to the users.

At the level of particular instruments, users assign substantial value to personal data protection instruments, such as objection to profiling or the right to data erasure (right to be forgotten), at the same time they largely underestimate the role of data portability – one of the key novel element of the GDPR reform[11]. From policy perspective this mechanism is of great importance as a potential game changer. Portability essentially lowers switching costs and shifts control over personal data to end-users. With portability, incumbent providers could no longer enjoy advantage resulting from exclusive use of large volumes of user-generated data. As a consequence, data portability opens scene for business models in which personal data is controlled and leased by the users instead of being a kind of currency to obtain money-free services[12].

We have also shown how the utility from particular instruments is affected by choice invariant characteristics of our respondents. Unsurprisingly, the preference for the right to be forgotten is higher among more privacy concerned individuals and lower for those respondents who actively use larger number of online services. Intensive online activity increases demand for informative and user-friendly privacy policies.

[11] The role of data portability might be as fundamental as the role of number portability in mobile telecommunications.

[12] Good example of such services are privacy management platforms, such as Hub-of-All-Things (HAT) or Cambridge Blockchain. They enable users to manage personal data from multiple accounts and services by storing it in a virtual container.

Our results on data portability can be treated as an early warning with regards to the adoption of this important tool. The success of this instrument will depend both on the greater user awareness as well as market response from new entrants offering innovative services.

ACKNOWLEDGMENTS

We are grateful to Brigitte Preissl, Roslyn Layton, Bertin Martens, participants of ITS 2017 Conference in Passau for their comments and discussions on the earlier versions of the paper. We gratefully acknowledge support from Digital Economy Lab at University of Warsaw.

APPENDIX

Table A1. List of attributes and their levels.

Attributes	Attribute levels	Measurement
INFDUTY	**EXTENDED: Wide scope of information duty, friendly form** Administrator informs in a comprehensive and detailed way about the aim and scope of personal data processing (via the infographic). Information about potential automated decision making is provided.	Categorical: value 1
	SQ: Narrow scope of information duty, legal form Administrator informs about the aim and scope of personal data processing; the form is not specified. There is no requirement to inform about automated decision making based on personal data.	Categorical: value 0 (baseline)
	REDUCED: No information duty	Categorical: value -1
PROFILING	**Right to object profiling** On demand of the user, his personal data cannot be processed for the profiling purposes	Dummy: value 1

	Lack of right to object profiling	Dummy: value 0
PORTABILITY	**Right to browse personal data and port between providers** User's personal data (photos, posts, personally identifying information) are available for browsing, downloading in the commonly used format and porting between online services providers	Dummy: value 1
	Right to browse personal data only User's personal data (photos, posts, personally identifying information) are available only for browsing	Dummy: value 0
FORGET	**EXTENDED: Right to correct and erase personal data** On user's demand her personal data are corrected or erased (unless it is against public interest)	Categorical: value 1
	SQ: Right to correct personal data User can apply for correction of his personal data	Categorical: value 0 (baseline)
	REDUCED: lack of right to correct or erase personal data	Categorical: value -1
INTERFACE	**Integrated privacy management within one app for all accounts** User is equipped with a management application unifying privacy management across all services.	Dummy: value 1
	Separate privacy management inside each account Privacy management is not unified and depends on the tools provided by individual providers	Dummy: value 0
COST	Monthly fee included in the internet subscription (in PLN)	Continuous on [0,15]. For SQ COST=0.

Table A2. Example of a choice card (translation)

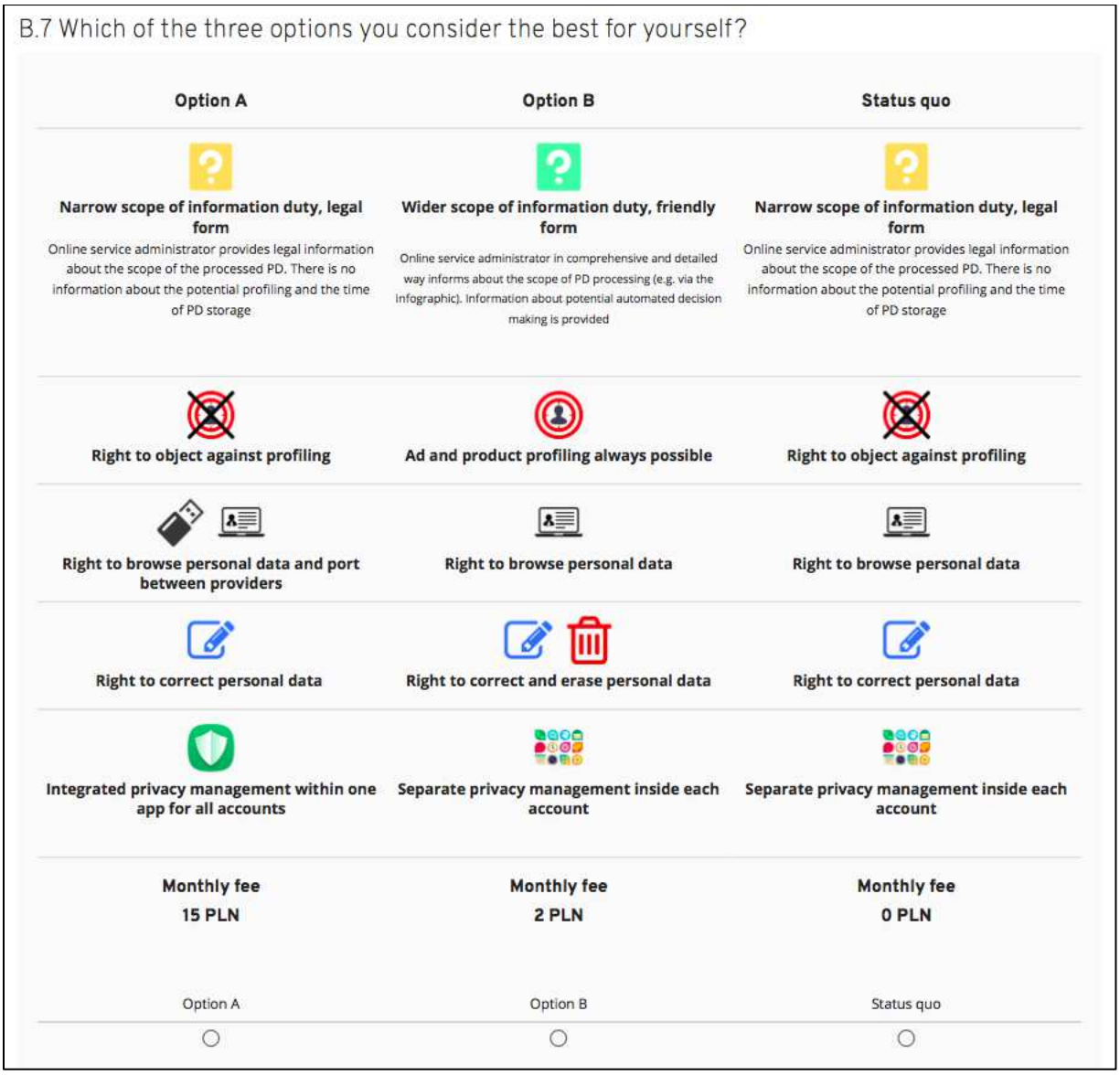
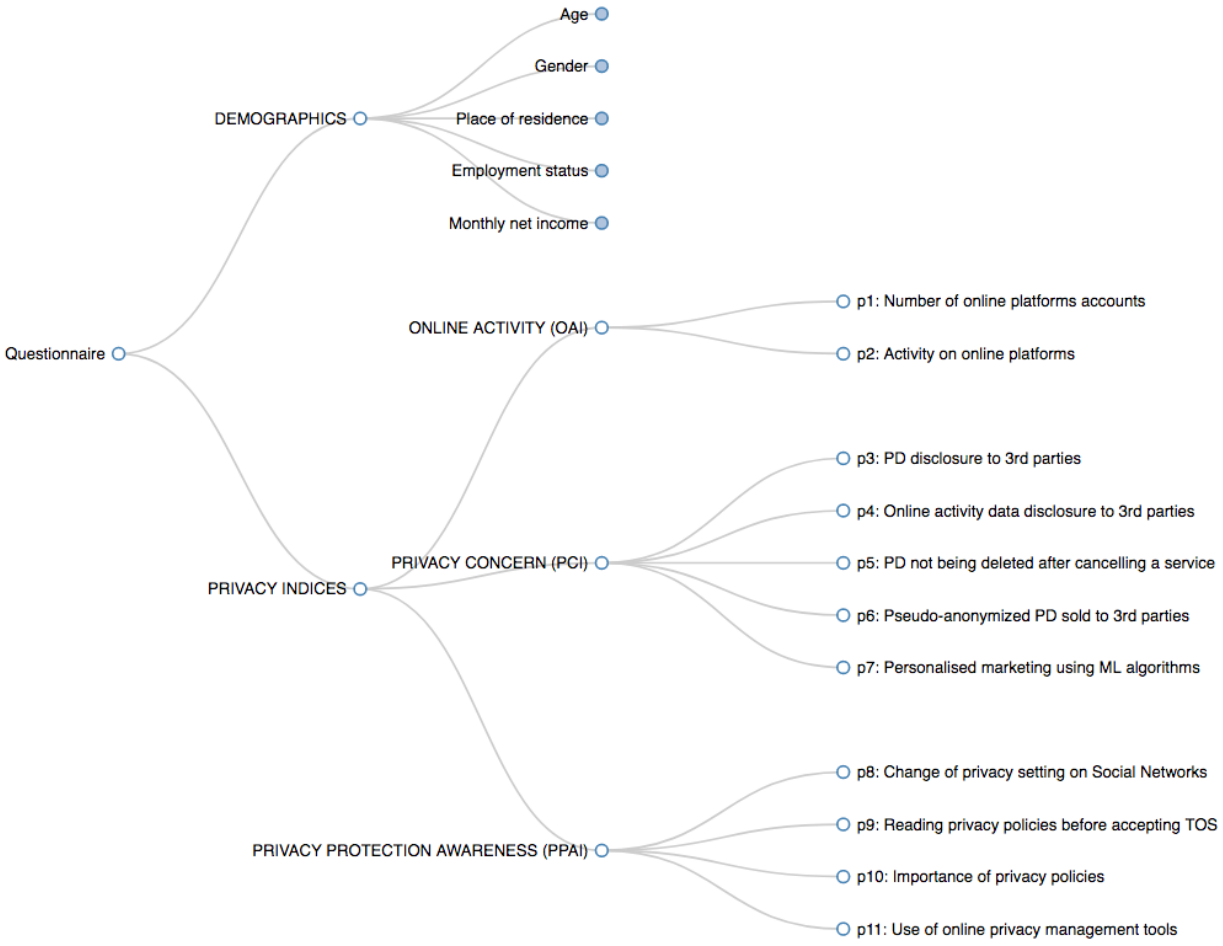


Table A3. Construction of indices.



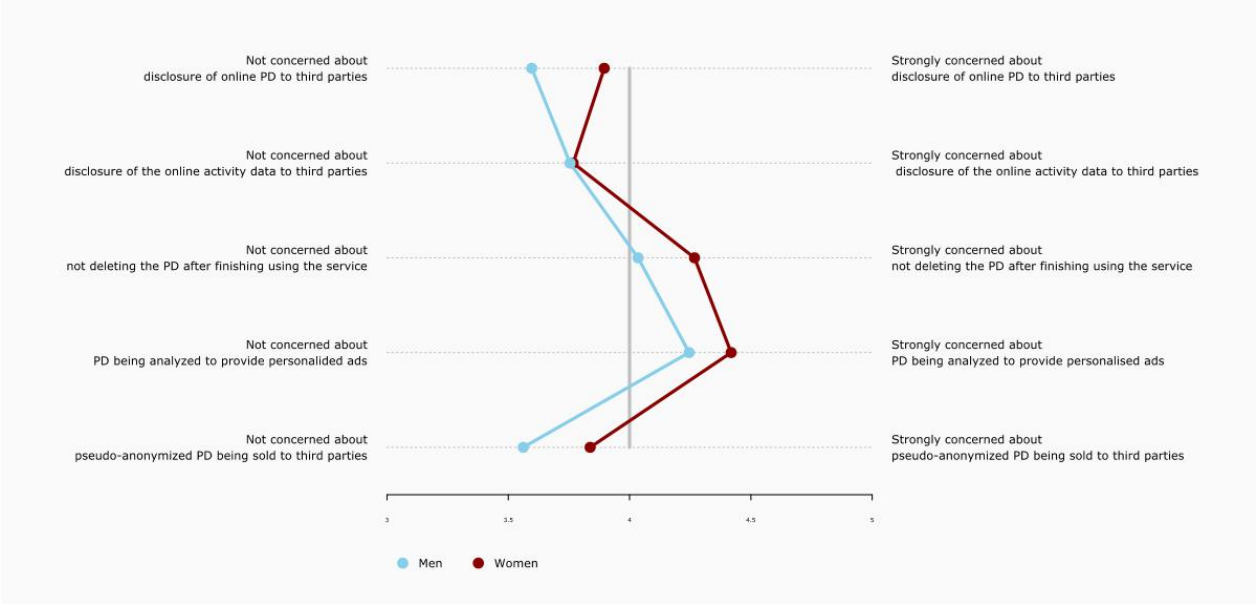
Question	Possible answers	Type	Mean	Index composition	Index
For which online service do you have an account?	Facebook, Twitter, LinkedIn, Instagram, WhatsApp, Skype, Pinterest, Snapchat	Multiple choice (equal weight)	6.6	$\sum_{i-1}^{8}(q1\_i * q2\_i)$ where: q1 platforms from question 1, q2 activity from question 2; normalized to discrete values	**Online Activity Index (OAI):** Measures presence and activity on online platforms and usage of online services

How often do you use the services from Q1?	(1) not at all – (2) at most few times a month – (3) at least once a week – (4) at least once a day – (5) more often than once a day	Likert-type scales (1:5)	3.3	[1:3]	
Have you ever changed the default privacy settings on social networks?	Yes, I have restricted the access to my content to selected users – Yes, I have restricted the personalized ads – Yes, I have changed the settings in other way – (0) No	Multiple choice (equal weight)	1.7	$\frac{\sum_{i=1}^{4} q\_i}{4}$ normalized to discrete values [1:3]	**Privacy Protection Awareness Index (PPAI):** Tracks knowledge about online privacy mechanisms and basic steps taken to control digital footprints.
Have you read the privacy policy before accepting the terms of use of the services from Q1?	(1) I have accepted without reading – (2) I have accepted after quick reading – (3) I have accepted after careful reading	Single choice	4.9		
Have you ever resigned from registration to an online service because	(1) Yes – (0) No	Single choice	0.65		

of its privacy policy?					
Have you ever managed your online privacy by using:	VPN (Virtual Private Network) – pseudonyms or fake personal data in the registration form – blocking or deleting cookies – ad-block apps – incognito mode while browsing – (0) I haven't ever used any of these options	Multiple choice (equal weights)	3.1		
To what extent would you be concerned about below situation? Your personal data (e.g. age, gender, location data) are disclosed to providers of online services which you don't use	1- I don't mind : 5-I would be strongly concerned	Likert-type scale (1:5)	3.8	$\frac{\sum_{i=1}^{5} q\_i}{5}$ normalized to discrete values [1:3]	**Privacy Concern Index (PCI):** Measures concerns about uncontrolled usage of online personal data by service providers and third parties
Information about your online activity (e.g. searched goods and services) is disclosed to providers of online services which you don't	1- I don't mind : 5-I would be strongly concerned	Likert-type scale (1:5)	3.8		

use					
Your personal data are not deleted after you finished using a service (e.g. after deletion of the online platform account)	1- I don't mind : 5-I would be strongly concerned	Likert-type scale (1:5)	4.2		
Your personal messages are analyzed by machine learning algorithms in order to provide you the personalized marketing	1- I don't mind : 5-I would be strongly concerned	Likert-type scale (1:5)	4.3		
Your pseudo-anonymized personal data is sold to third parties	1- I don't mind : 5-I would be strongly concerned	Likert-type scale (1:5)	3.7		

Fig. A4. Privacy Concern Index mean results for gender subgroups.



Note: PD – personal data; Scale: 1 – I don' mind, 5 = I would be strongly concerned.

BIBLIOGRAPHY

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What Is Privacy Worth? *The Journal of Legal Studies, 42*, 2.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature, 54*(2), 442-492.

Awad, N. F., Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly, 30*(1), 13–28.

Bankston, K. (2009). Facebook's New Privacy Changes: The Good, The Bad, and The Ugly'Electronic Frontier Foundation, 9 December 2009.

Bauer, C., Korunovska, J., & Spiekermann, S. (2012). On the value of information-what Facebook users are willing to pay. *ECIS 2012 proceedings*.

Ben-Akiva, M., Bradley, M., Morikawa, T., Benjamin, J., Novak, T., Oppewal, H., & Rao, V. (1994). Combining revealed and stated preferences data. *Marketing Letters, 5*(4), 335-349.

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters, 117*(1), 25-27.

Bliemer, M. C., & Rose, J. M. (2013). Confidence intervals of willingness-to-pay for random coefficient logit models. *Transportation Research Part B: Methodological, 58*, 199-214.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the Association for Information Science and Technology, 58*(2), 157-165.

Butler, S., & Garrett, G. (2014). The Value of Personal Information to Consumers of Online Services: Evidence from a Discrete Choice Experiment.

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & de Oliveira, R. Your browsing behavior for a big mac: Economics of personal information online. In *Proceedings of the 22nd international conference on World Wide Web, 2013* (pp. 189-200): ACM

Carson, R. T., Flores, N. E., Martin, K. M., & Wright, J. L. (1996). Contingent Valuation and Revealed Preference Methodologies: Comparing the Estimates for Quasi-Public Goods. *Land Economics, 72*(1), 80-99.

Carson, R. T., Groves, Th., List, J., A. (2014), Consequentiality: A Theoretical and Experimental Exploration of a Single Binary Choice, Journal of the Association of Environmental and Resource Economists, Vol. 1, No. 1/2.

Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *BCL Rev., 55*, 93.

Cvrcek, D., Kumpost, M., Matyas, V., & Danezis, G. A study on the value of location privacy. In *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, 2006* (pp. 109-118): ACM

Danezis, G., Lewis, S., & Anderson, R. J. How much is location privacy worth? In *WEIS, 2005* (Vol. 5)

Dix, A., Thüsing, G., Traut, J., Christensen, L., Etro, F., Aaronson, S. A., & Maxim, R. (2013). EU data protection reform: Opportunities and concerns. *Intereconomics, 48*(5), 268-285.

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There's a price for that. In *The economics of information security and privacy* (pp. 211-236): Springer.

European Commission (2015). Special Eurobarometer 431. Data protection.

European Commission (2017). Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World.

European Parliament (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Greene, W. H. (2011). *Econometric Analysis* (7ed.). Upper Saddle River, NJ: Prentice Hall.

Greene, W. H., & Hensher, D. A. (2007). Heteroscedastic Control for Random Coefficients and Error Components in Mixed Logit *Transportation Research Part E: Logistics and Transportation Review, 43*(5), 610-623.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*(2), 13-42.

Hann, I.-H., Hui, K.-L., Lee, T., & Png, I. (2002). Online information privacy: Measuring the cost-benefit trade-off. *ICIS 2002 proceedings*, 1.

Hensher, D., & Greene, W. (2003). The Mixed Logit model: The state of practice. [10.1023/A:1022558715350]. *Transportation, 30*(2), 133-176.

Holland, H. B. (2009). Privacy Paradox 2.0. *Widener LJ, 19*, 893.

Johnson, B. (2010). Privacy no longer a social norm, says Facebook founder. *The Guardian, 11*(01).

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

Krasnova, H., Hildebrand T., Guenther O. (2009). Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis, ICIS 2009 Proceedings. Paper 173.

Krinsky, I., & Robb, A. L. (1986). On approximating the statistical properties of elasticities. *The Review of Economics and Statistics*, 715-719.

McFadden, D. (1974). Conditional Logit Analysis of Qualititative Choice Behaviour. In P. Zarembka (Ed.), *Frontiers in Econometrics* (pp. 105-142). New York, NY: Academic Press.

OECD (2013). Exploring the economics of personal data: A survey of methodologies for measuring monetary value. *Digital Economy Papers 220 (2013)*: OECD.

Patil, S., et al. (2015), Public Perception of Security and Privacy: Results of the comprehensive analysis of PACT's pan-European Survey. PACT Project Consortium.

Png, I. P. (2007). On the value of privacy from telemarketing: evidence from the'Do Not Call' registry.

Potoglou, D., Dunkerley, F., Patil, S., & Robinson, N. (2017). Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study. *Computers in Human Behavior, 75*, 811-825.

Potoglou, D., Palacios, J.-F., & Feijóo, C. (2015). An integrated latent variable and choice model to explore the role of privacy concern on stated behavioural intentions in e-commerce. *Journal of choice modelling, 17*, 10-27.

Preibusch, S. (2015). The Value of Web Search Privacy. *IEEE Security & Privacy, 13*(5), 24-32.

Sándor, Z., & Wedel, M. (2001). Designing Conjoint Choice Experiments Using Managers' Prior Beliefs. *Journal of Marketing Research, 38*(4), 430-444.

Street, D. J., & Burgess, L. (2007). *The Construction of Optimal Stated Choice Experiments: Theory and Methods*: Wiley-Interscience.

Train, K. E. (2009). *Discrete Choice Methods with Simulation*. New York: Cambridge University Press.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254-268.

Varian, H., Wallenberg, F., & Woroch, G. (2005). The demographics of the do-not-call list [security of data]. *IEEE Security & Privacy, 3*(1), 34-39.

World Bank (2018). Data retrieved March 15, 2018, from World Development Indicators Online (WDI) database (indicator: IT.NET.USER.ZS).

Whitehead, J. C., Phaneuf, D. J., Dumas, C. F., Herstine, J., Hill, J., & Buerger, B. (2010). Convergent Validity of Revealed and Stated Recreation Behavior with Quality Change: A Comparison of Multiple and Single Site Demands. *Environmental and Resource Economics, 45*(1), 91-112.