University of Warsaw
Faculty of Economic Sciences

Working Papers
No. 17/2017 (246)

How much consumers value on-line privacy? Welfare assessment of new data protection regulation (GDPR)

Maciej Sobolewski
Michał Paliński

Warsaw 2017

UNIVERSITY OF WARSAW
Faculty of Economic Sciences

How much consumers value on-line privacy? Welfare assessment of new data protection regulation (GDPR)

MACIEJ SOBOLEWSKI
Joint Research Center, European Commission
Digital Economy Lab
Faculty of Economic Sciences
University of Warsaw
e-mail: maciej.sobolewski@uw.edu.pl

MICHAŁ PALIŃSKI
Digital Economy Lab
Faculty of Economic Sciences
University of Warsaw
e-mail: m.palinski@delab.uw.edu.pl

Abstract

Our paper analyses upcoming 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 General Data Protection Regulation and assess potential welfare gain from this policy intervention. On methodological grounds, we utilize stated preference discrete choice experiment. Our final dataset consisted of 4390 choices made by 143 respondents. We used these data to estimate the mixed logit model. Our study for the first time analyses the broader spectrum of 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 instruments, such as right to be forgotten, right to object profiling and personal data portability. The main finding from the analysis is that implementation of enhanced privacy control mechanisms will generate positive welfare effect. The size of estimated welfare gain from policy intervention of the same scope as 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 data as well as shortage of effective tools for privacy management.

Keywords:
personal data management, e-privacy, General Data Protection Regulation, mixed logit

JEL:
C25, D12, L51

Acknowledgements
This paper is an outcome of research project undertaken within Digital Economy Lab at University of Warsaw. It 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.

JEL:
https://doi.org/10.26405/WP/WNE/2017/246/017

1. Introduction

The current legal basis for privacy protection in the EU has been adopted over 20 years when less than 1% of global population was using the Internet (Directive 95/46). Not surprisingly, in times of Web 2.0 and data-driven economy this framework has been perceived as not adequate. Therefore the EU member states agreed upon the necessity of implementing major reform regarding data protection framework. The rationale for the new regulation - General Data Protection Regulation (GDPR) is to shift the balance of power and control over personal information from online providers to end users.

GDPR extends the scope of informative obligations on service providers and grants several protection instruments to users, such as: (i) right to data browsing and erasure, (ii) objection to automated processing, (iii) portability of data and (iv) objection to profiling (European Parliament 2016). 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 such as activity data or shopping lists. Among novel elements, GDPR enforces privacy by design and privacy by default. Under these two principles, explicit consent to data processing for each specified purpose is required from the user and it can be asked only for purposes that are critical for operation of a service. Moreover, service providers must set maximal protection level as a default setting in privacy policies.

Despite obvious benefits from sharing personal data online, behavioural studies document serious concerns related to potential abuse of such data (like hidden influence or manipulation) and insufficient protection of privacy, both arising 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 are not consistent with real behaviour of users who often disclose personal data for quite small benefits or discounts. This ambivalent attitude, known as privacy paradox is explained with lack of proper instruments to control the utilization of personal data on the Internet. In this light GDPR can be viewed as a policy response to this shortage. To what extent the new regulation is beneficial to Internet users? Which instruments have the greatest value and hence potential for wide adoption? These are the two open questions, which we address in this study.

Our paper analyses upcoming 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 the new regulation is coming into force on the 25th of May 2018, our evaluation has essentially ex ante character. On methodological grounds, we utilize stated preference discrete choice experiment as we do not yet observe any impacts of GDPR on real behaviour. This is a common approach in empirical research on privacy economics because revealed preference data is proprietary. Existing empirical work focuses mainly on estimating the value of personal data. Our study for the first time analyses the broader spectrum of 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 instruments, such as right to be forgotten, right to object profiling and personal data portability.

This paper is organized in two main sections. In section 2 we briefly review literature on behavioural aspects of privacy and provide some evidence on users' attitudes towards privacy protection based on Eurostat data. In section 3 we provide empirical assessment of welfare benefits from implementation of the main protection mechanisms envisaged by GDPR. Section 4 concludes.

2. Literature review

The EC justifies the new data regulation to a large extent with people's privacy concerns (European Commission 2017).[1] But do Internet users really care about having control over personal information they share online? Surveys and polls show that indeed online privacy is 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 (see Figure 1). On the other hand, experimental studies indicate that individuals tend to reveal their personal data for quite small remuneration (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 (see: Figure 1). Such inconsistency between declared concerns and the actual behaviour marks the ambivalence in the attitude towards privacy, known as 'privacy paradox'. It is a well-established concept in the social sciences which gained a lot of attention from empirical researchers in the recent years (Holland 2009). The data from Figure 1 supports the hypothesis about the existence of privacy paradox in the EU, at least in central and southern member states (combination of higher scores on the left pane and lower scores on the right pane). If concerns over online privacy have merely declarative nature it could weaken the argumentation in favour of strengthening the users' control over their personal data. However, there is a strong empirical evidence that users substantially value their personal data, which points to the importance of online privacy.

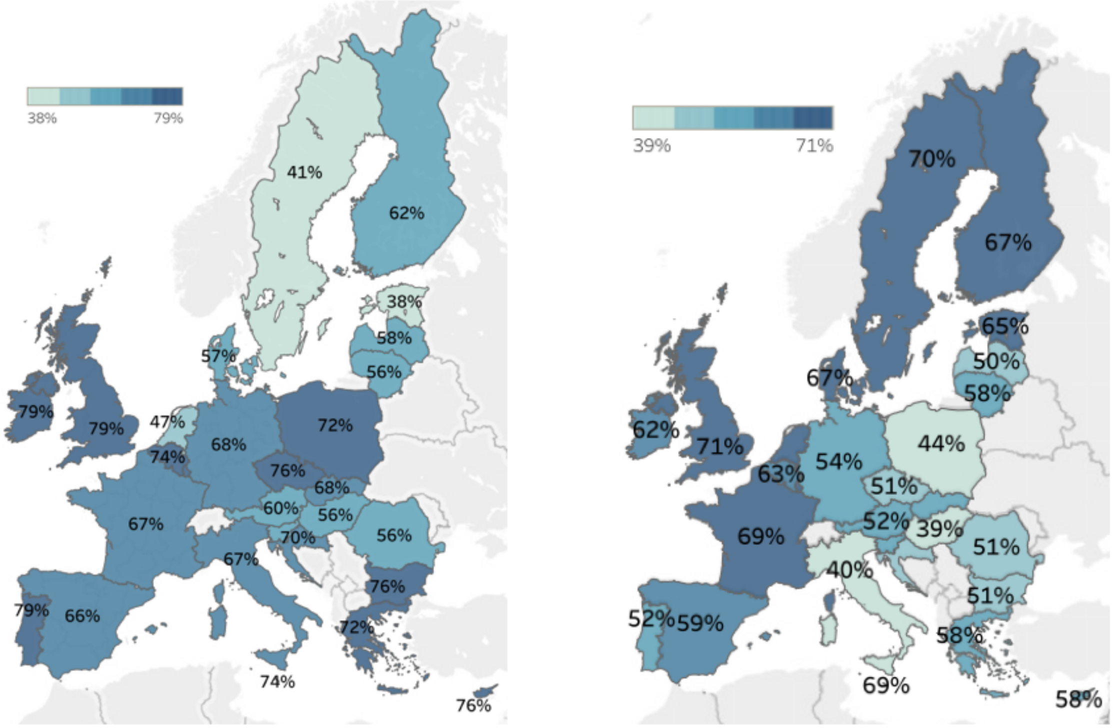
The economics of privacy starts with the observation that 'personal data have been commodified into a tradeable asset' (Preibusch 2015). Research body in privacy economics is growing fast since early 2000s, following rapid development of the Internet and proliferation of business models based on intensive processing of personal data acquired via online interactions (Acquisti et al. 2016). A handful methodologies are commonly deployed in determining the monetary value of personal data. Two general 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 personal data based on actual purchase transactions. This revealed preference data can be used to examine a trade-off between privacy and remuneration or enhanced service functionality. 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 personal data in the specific context for which revealed preference data is not available or non-existent (as in case of GDPR).

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

In the Table 1 we provide the summary of the main empirical studies which derive valuations for personal data: willingness-to-pay (WTP) for protection and willingness-to-accept (WTA) for disclosure. The majority of both WTP and WTA studies focus on assessment of single privacy enhancing mechanism. Among WTP studies there is a strand of research dealing with the monetary value estimation of users' 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).

Figure 1. A glance on privacy paradox across EU.

Left pane: 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: 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).



Note: $n_{left} = 16244$; $n_{right} = 15339$

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

Table 1 Studies measuring the valuation of online personal data.

(A) Willingness-to-pay (WTP) for not disclosing the personal data

Count	Study	Type of	Object of	Main results

ry		study	valuation	
EU 27	Potoglou et al. (2017)	DCE	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 above 5k EUR. 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	Protection from secondary use of personal data	WTP to avoid sharing personal data (PD) with third parties: 5.57GBP per transaction; value of not storing PD by online retailer: 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	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	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	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.
FR, DE, UK, RU	Krasnova et al. (2009)	DCE	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	Protection from telemarketing	WTP for avoiding telemarketing by signing in to the federal 'do not call registry': 8.3USD annually.
US	Hann et al. (2007)	DCE	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	Tsai et al. (2011)	Lab experiment	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).
US	Varian et al. (2005)	Market valuation	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	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 online personal data.

Country	Study	Type of study	Object of valuation	Main results
ES	Carrascal et al. (2013)	Field experiment (reverse second price auction)	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	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)	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)	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.

Source: Own elaboration.

Evidence from the studies listed in Table 1-A suggests that the willingness-to-pay for not disclosing personal data is rather noticeable. On the other hand users are willing to reveal their personal information for a relatively small reward (see the studies listed in Table 1-B). In this light how can we reconcile the concerns about protection of online privacy with the users’ common nonchalance with respect to online privacy management? Perhaps the answer is simple.

Although Internet users in the EU are evidently concerned about the risk of leakage of sensitive data and are under the 'veil of ignorance' as to what is being collected, they do not have instruments to control the scope and use of their personal data. Without access to user friendly and effective tools a disclosing behaviour such as selling personal data for small remuneration might be a rational decision. GDPR can alter this state of affairs by equipping Internet users with the a set of tools for personal data control. If this is the case, then particular mechanisms such as right to be forgotten, increased information duties, right to object profiling and personal data portability should generate substantial value to the users leading to positive welfare effect from policy intervention.

3. Economic valuation of GDPR

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 privacy control mechanisms will generate positive welfare effects. We estimate the change in consumer surplus resulting from implementation of 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 GDPR.

3.1. Data

The sample used in the study is composed of 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 internet users, who usually have several accounts on different online platforms. Knowledge about preferences of digital natives towards protecting personal data is particularly meaningful, because they face privacy related trade-offs on everyday basis. Undoubtedly, this group is affected by any kind of privacy regulation, which adds to the reliability of collected data.

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 scope.[2] 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).[3] 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 Annex 1.

[2] For example, the information obligation or right to be forgotten could assume narrow or wider scope, while portability of data or right to be forgotten was measured on a zero-one scale

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

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 interventions, hence no actual data exists yet.

3.1.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:

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

where $\boldsymbol{\beta}$ is the vector of utility parameters, $\mathbf{x}$ 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 $\boldsymbol{\beta}_i \sim f\ (\mathbf{b}, \boldsymbol{\Sigma})$, where $\mathbf{b}$ 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 $\mathbf{b}, \boldsymbol{\Sigma}$ can be obtained numerically from maximization of the following log-likelihood function:

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

where y_{ijt} 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.[4]

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

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):

$$WTP_k = \frac{\beta_k}{\beta_{price}} \qquad (3)$$

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 derive simulated change in consumer surplus from introduction of 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).

3.2.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):

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

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 2 below. We set FORGET_SQ and INFDUTY_SQ as a 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 2. 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** **(s.e.)**	**Standard deviation** **(s.e.)**
INFDUTY_E - extended scope of information duty relative to SQ (n)	0.880*** (0.156)	1.016*** (0.217)
INFDUTY_R – reduced scope of information duty relative to SQ (n)	-1.006*** (0.2326)	1.201*** (0.273)
PROFILING – right to object profiling (n)	0.865*** (0.147)	1.139*** (0.214)
PORTABILITY – right to port personal data (n)	-0.197 (0.135)	0.934*** (0.204)
FORGET_E – extended right to be forgotten compared to SQ (n)	1.267*** (0.168)	0.997*** (0.234)
FORGET_R – reduced right to be forgotten relative to SQ (n)	-1.026*** (0.197)	1.088*** (0.255)
INTERFACE – integrated privacy management (n)	0.381*** (0.135)	0.832*** (0.228)
(minus) COST – monthly fee (ln)	-1.778*** (0.116)	1.494*** (0.146)
Model characteristics		
Log-likelihood	-1,038.106	
n (observations)	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, 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 3 we present median WTP estimates in our sample, based on MXL coefficients.

Table 3. Willingness to pay for privacy policy characteristics [PLN].[5]

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

	Gross consumer surplus per capita (s.e.)	**95% c.i.**
implementation of 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

[5] 1 PLN ≈ 0.25 EUR

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 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 over the distribution of willingness to pay for the implementation of 'GDPR policy alternative'. It equals 6.5 EUR in per capita terms per month. We consider this level as substantial, given that the monthly price for broadband access in Poland is around 10-12 EUR.

4. Conclusion

In 2010 Facebook aroused controversy by introducing new default privacy settings for its 350m users[6]. 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).[7] 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 fuelled 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 favour 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 will be mitigated by new regulation on data protection? This study address this question by providing an insight into preferences of a group of digital natives from Poland.

The main finding from the analysis is that implementation of enhanced privacy control mechanisms will generate positive welfare effect. The size of estimated welfare gain from policy intervention of the same scope as 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 data as well as shortage of effective tools for privacy management. In this respect GDPR might be seen as a proper policy response to the 'privacy paradox'.

While end-users assign substantial value to personal data protection instruments, such as objection to profiling or the right to data erasure (also known as the right to be forgotten), at the same time they largely underestimate the role of data portability – one of the key novel element of GDPR reform.[8] From policy perspective this mechanism is of great importance as a potential

[6] In the Q1 2017 Facebook had already 1.9 bln active users.

[7] 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.

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

game changer. Portability essentially lowers switching costs and shifts control over personal data to end-users. Incumbent providers will 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.[9]

Our results on data portability can be treated as an early warning with regards to the effective implementation of the entire scope of GDPR. Hence, of particular importance is keeping this instrument unrestricted and user friendly to the broadest possible extent.

This research can be extended in two directions. First, it would be worthwhile to replicate similar experiment on larger and representative sample to obtain more precise assessment of valuations and welfare effects. Secondly, our study unveiled significant preference heterogeneity, which can be explored with observed characteristics and attitudes of respondents, adding more detailed picture of factors that influence valuation of personal data protection mechanisms.

[9] 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.

5. References

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.

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.

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., 2013. Your browsing behavior for a big mac: Economics of personal information online. In Proceedings of the 22nd international conference on World Wide Web, 189-200.

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.

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

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

Danezis, G., Lewis, S., & Anderson, R. J., 2005. How much is location privacy worth? WEIS, 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. The economics of information security and privacy, 211-236.

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).

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K., 2009. Privacy concerns and identity in online social networks. Identity in the Information Society, 2(1), 39-63.

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.

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.

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.

6. Annex

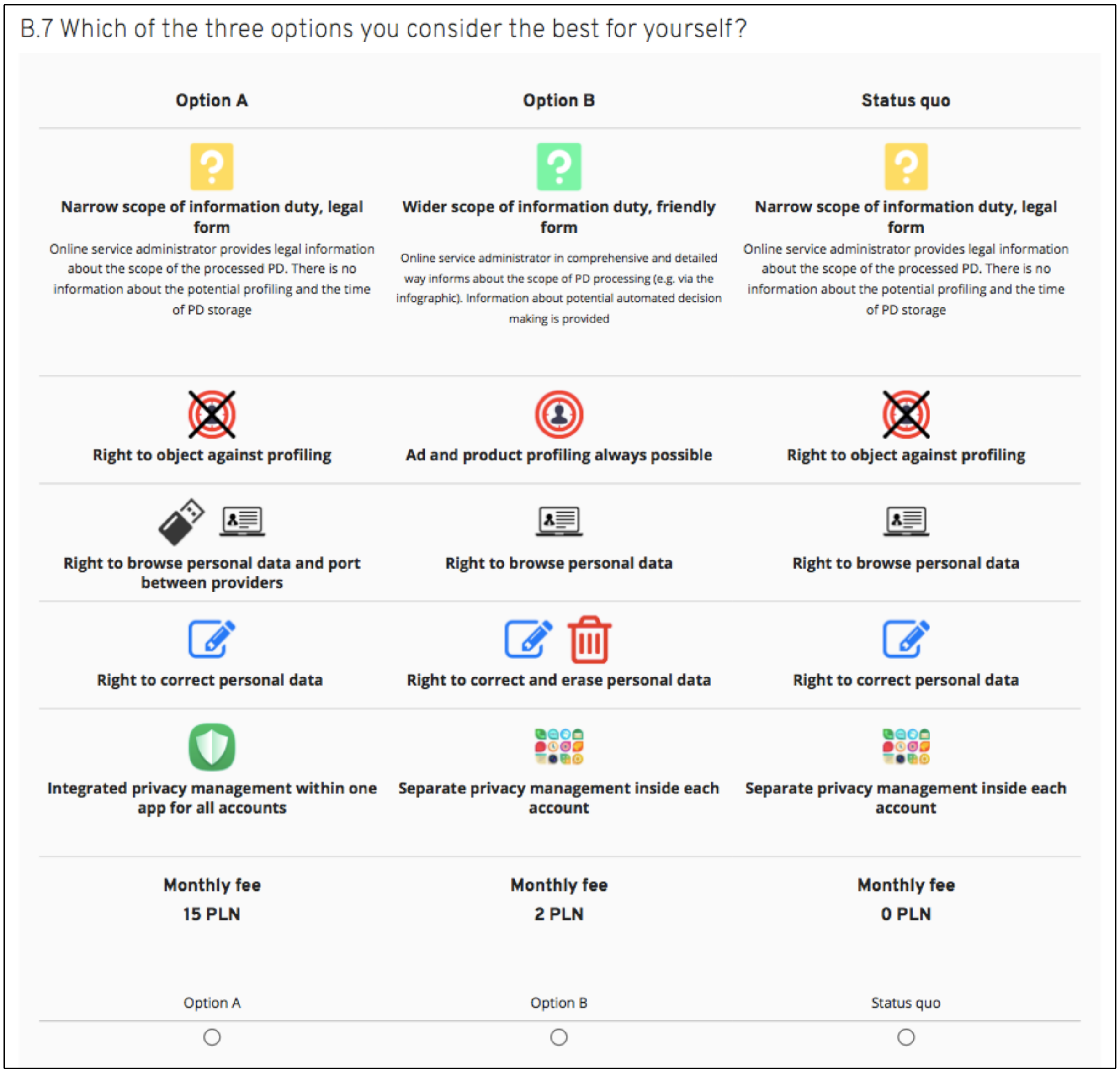
Table A1. List of attributes and their levels.

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	Categorical: value

	personal data	-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.

Source: Own elaboration.

Table A2. Example of a choice card (translation)



B.7 Which of the three options you consider the best for yourself?

Option A	Option B	Status quo
Narrow scope of information duty, legal form Online service administrator provides legal information about the scope of the processed PD. There is no information about the potential profiling and the time of PD storage	**Wider scope of information duty, friendly form** Online service administrator in comprehensive and detailed way informs about the scope of PD processing (e.g. via the infographic). Information about potential automated decision making is provided	**Narrow scope of information duty, legal form** Online service administrator provides legal information about the scope of the processed PD. There is no information about the potential profiling and the time of PD storage
Right to object against profiling	**Ad and product profiling always possible**	**Right to object against profiling**
Right to browse personal data and port between providers	**Right to browse personal data**	**Right to browse personal data**
Right to correct personal data	**Right to correct and erase personal data**	**Right to correct personal data**
Integrated privacy management within one app for all accounts	**Separate privacy management inside each account**	**Separate privacy management inside each account**
Monthly fee **15 PLN**	**Monthly fee** **2 PLN**	**Monthly fee** **0 PLN**
Option A	Option B	Status quo
○	○	○

Source: Own elaboration.

Faculty of Economic Sciences
University of Warsaw
44/50 Długa St.
00-241 Warsaw
www.wne.uw.edu.pl