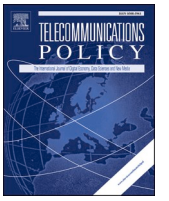
Telecommunications Policy 46 (2022) 102308

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol



Your privacy for a discount? Exploring the willingness to share personal data for personalized offers[1]

Frode Alfnes [a,c], Ole Christian Wasenden [a,b,*]

[a] School of Economics and Business, Norwegian University of Life Sciences, Norway
[b] Telenor Research, Norway
[c] Consumption Research Norway, Oslo Metropolitan University, Norway

ARTICLE INFO

JEL classification:
C83
D82
D83
M37

Keywords:
Personal data
Preference elicitation
Data privacy
Mobile (cell) phone services

ABSTRACT

This paper explores how willing consumers are to share personal data to receive personalized offers on their mobile (cell in the US) phones using nationwide surveys of mobile users, 16–35 years old, in Norway, Serbia, Malaysia, and Pakistan. We ask respondents about the likelihood they would use three types of personalized advertising services delivered through their mobile operator, with services varying with respect to the level of personal data collected and whether shared with third parties. In all four countries, respondents state that their likelihood of using a personalized ad service decreases when the service uses more personal data or shares the data with third parties. Using a split sample design, we find that introducing a 10% discount on mobile subscriptions for those using the ad service increases the stated likelihood of using the service. We find significant differences in willingness to share personal data attitudes between countries, with respondents in high-income Norway being least willing and those in low-income Pakistan most willing to share personal data. We identify only minor differences between respondents in Serbia and Malaysia, middle-income countries in Europe and Asia. The study contributes to the literature on the willingness to share personal data by including young adult respondents from countries in both Europe and Asia. Furthermore, framing the survey questions in a mobile service context is appreciably closer to telecom reality than most existing experimental studies on sharing of personal data.

1. Introduction

Imagine you are out shopping and a message lands on your mobile (cell in the US) phone. It contains an offer from a nearby store, tailored to match your interests. How do you feel? Today's technologies make it possible to combine knowledge of consumer preferences and detailed location data to target nearby potential customers with personalized offers on their mobile devices. However, consumers must give up some of their privacy and share personal data with commercial actors to receive such personalized offers. To explore the privacy-personalization tradeoff in a telecom setting, this paper investigates factors affecting mobile users' interest in mobile services using location data and browsing history to create personalized offers. We utilize survey data from a large telecommunications firm with business units in Europe and Asia. We study the privacy preferences of mobile users in Norway, Serbia,

[1] This research was supported by a grant from the Research Council of Norway.
* Corresponding author. School of Economics and Business, Norwegian University of Life Sciences, Norway.
E-mail address: olwa@nmbu.no (O.C. Wasenden).

https://doi.org/10.1016/j.telpol.2022.102308
Received 9 July 2021; Received in revised form 11 January 2022; Accepted 15 January 2022
Available online 7 February 2022

Malaysia, and Pakistan and investigate the country differences in the stated willingness to share location and browsing history with commercial actors to receive personalized offers.

The increasing use of smartphones and mobile Internet connections has significantly improved the possibility of collecting and using location and personal information from mobile users worldwide. Many online companies are part of the personal data ecosystem, and data on users are essential to their business (Chaudhry et al., 2015). These companies often operate in two-sided markets, selling data or ads space to advertisers and services and products to end-users (Acquisti et al., 2016). Google's Chief Economist Hal Varian (2010, 2014) describes the benefits of this development along four dimensions: more efficient data extraction and analysis, possibilities for personalization and customization of goods and services, easier to conduct experiments, and new kinds of contracts due to better monitoring.

The large amounts of data that online companies harvest result in a growing concern about privacy. Zuboff (2015) comments on Varian's benefits and states that they depend on an implicit logic of surveillance. Acquisti et al. (2020) argue that even when users of digital services take many steps to protect their privacy, they will unlikely attain desired levels. In response to these challenges, several countries have implemented laws and regulations to give citizens better control over their data, e.g., the European Union's General Data Protection Regulation and Japan's Act on the Protection of Personal Information (Schwartz, 2019). Among academics, we have seen a growing literature on consumer privacy preferences (Acquisti et al., 2015, 2020) and personalized ads and services (e.g., Segijn et al., 2021; Strycharz et al., 2019; Tucker, 2014).

A much-studied question in privacy research is whether consumers place a positive value on privacy and personal data. Related to this is the so-called privacy paradox that states that people claim they worry about digital privacy but do not act on their worries. A literature review by Kokolakis (2017) on the privacy paradox suggests mixed results. Some studies find that most consumers are unwilling to pay for privacy (e.g., Beresford et al., 2012), while others find that most consumers place some positive value on their privacy (e.g., Benndorf & Normann, 2018). In a recent review of the privacy literature, Acquisti et al. (2020) argue that ample evidence exists that people are both concerned about their privacy and take actions to protect it, even though it is not evident in all circumstances.

Acquisti et al. (2020) point out that most of the research on privacy is done in WEIRD (Western, Educated, Industrialized, Rich, and Democratic) countries. The usage of digital services that collect large amounts of personal data and the potential challenge that follows are not limited to the WEIRD countries. For example, the share of the population using Facebook are as high in several non-WEIRD countries as typically seen in WEIRD countries. According to NapoleonCat,[1] close to 86 percent of the population in Malaysia used Facebook in 2021, while the number for Norway, the WEIRD country in our study was 75 percent. Similar numbers for the two other non-WEIRD countries in our study are 52 percent in Serbia and 24 percent in Pakistan. To help reduce the knowledge gap of privacy preferences in non-WEIRD countries, we compare privacy attitudes in three non-WEIRD countries, Malaysia, Pakistan, and Serbia, with attitudes in Norway, a WEIRD country.

Several studies have investigated scale and scope sensitivity in privacy preferences regarding the amount of data the participants shared (scale effects) and how many they share it with (scope effects). For example, Benndorf and Normann (2018) elicit reservation prices for various bundles of personal data. They identify significant scope sensitivity when they ask participants to share contact and preference data, but not when they ask them to share different bundles of Facebook data. Schudy and Utikal (2017) find that German students' willingness to share personal data with anonymous recipients decreases with the number of recipients. However, they discover no scale effect arising from the amount of data each unknown recipient receives. These mixed results suggest the need for more research into scale and scope sensitivity in privacy preferences.

As the Internet became more widespread, the possibility of gathering personal data about consumers increased, and marketing academics started to investigate its effect on marketing practices. Several studies pointed to an expected increase in the use of personalization. Peppers et al. (1999) describe how a business could increase the value of its customer base through one-to-one marketing. Companies should change their marketing strategies and base them on what they know about the individual customer. Spiekermann et al. (2001) state that "Long existing dreams of one-to-one marketing are close to coming true …". O'Malley et al. (1997) discuss businesses using personal data in their market activities and conclude that what marketeers call "intimacy" consumers could see as "intrusion". Hence, the literature on the balancing act of delivering good, personalized services and ads without invading the consumers' privacy is more than two decades in the making.

It is now possible for online ads to be personalized and tailored to specific users at specific times and in particular locations (Chen & Hsieh, 2012). The tailoring can make ads more relevant for the receiver (De Keyzer et al., 2015). However, depending on how well the ads meet consumer preferences, they could be entertaining, informative or even irritating (Haghirian et al., 2008). Reviewing the current state and future of advertising research, Taylor and Carlson (2021) conclude that the advertising field has recently seen dramatic changes from technology advancements and new media consumption patterns. Increased understanding of the impact of these changes and further developments, including developments in privacy issues, still need more research.

Privacy concerns, privacy knowledge, and trust are often included in studies of online privacy behavior (Acquisti et al., 2016, 2020; Baruh et al., 2017; Evjemo et al.[2] 2020). We also use these attitudes and define them as done in the privacy and trust literature. Taylor et al. (2009) define privacy concern as a customer's concern for controlling the acquisition and subsequent use of information generated or acquired in online transactions. Trepte et al. (2015) split privacy knowledge into declarative knowledge - to understand risks and rights - and procedural knowledge - to understand how to protect personal data. In our study, we focus on declarative

[1] https://napoleoncat.com.

[2] Evjemo et al. (2020) explore the knowledge and concern measures used in this paper.

knowledge. Rosenthal et al. (2020) discuss trust in a digital setting and follow the definition of Mayer et al. (1995). They define trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al., 1995, p. 712). All three factors play a role in forming peoples' privacy attitudes and behavior, and they are relevant as control variables in our study (Baruh et al., 2017; Brown & Muchira, 2004; Chellappa & Sin, 2005; Wang et al., 2016; Youn, 2009).

To shed light on consumers' privacy behavior and valuation of privacy in non-WEIRD countries, we ran a survey experiment of young mobile Internet users in Serbia, Malaysia, and Pakistan and compared them to young mobile Internet users in Norway. As part of the survey experiment, we presented three versions of a personalized ad service and asked respondents to express their likelihood of using this service in a hypothetical scenario. The core of the service was that users will receive up to 10 ads a month via text messages that are personalized based on information the user chooses to share. We showed respondents three different variations of the ad service. The most basic version of the service only used location data. The next version of the service combined the location data with the browsing history. Notably, only the mobile operator receives the data for both the first and second service versions. The last version of the service combined location and browsing history and shared the information with the mobile operator and a third-party store. For half the participants, we described the ad services as including a 10% discount on their mobile subscription.

We identify scale and scope sensitivity regarding the amount of data shared and how many receive the data. While the stated likelihood of participants using the personalized ad service decreases when the mobile operator requests more personal data or shares the data with a third party, introducing a 10% discount on the mobile subscription for those using the ad service increases the likelihood of using the service. We identify significant effects of concern, knowledge, and trust on the respondents' willingness to use the services. Comparing results across countries, we reveal substantial differences in these stated attitudes, with respondents in Norway being least willing and those in Pakistan most willing to share personal data, adding a geographical aspect to the heterogeneity of consumers.

2. Method

The privacy questions were included in a survey exploring mobile Internet usage conducted by a large European telecommunication firm in countries where they had business units in 2017. The surveyed contries were Norway, Serbia, Malaysia, and Pakistan, and the data collection was conducted by Kantar TNS, a leading global market research agency. Here, we describe the survey design, sample, and behavioral predictions related to privacy.

2.1. Design of survey experiment

The privacy survey experiment uses a split-sample design and three hypothetical survey questions. We ask respondents about how likely it is that they will use different services with specific characteristics using the question: "Consider the following service. How likely is it that you would use such a service?" with responses on a five-point scale (very likely, likely, neutral, unlikely, very unlikely).

We use a 3×2 experimental design with a mix of within- and between-sample treatments. The experiment includes three levels of data sharing and two levels of discount, zero and 10%. The data-sharing factor is a within-sample factor where the respondents see all three levels, starting with the level where least data is shared. The discount factor is a between-sample factor, where we randomly draw respondents into one of the two treatments. In addition to these two experimental design factors, the four countries are between-sample factors.

The data-sharing factor is operationalized through services where the respondents receive a personalized offer from stores they pass or visit. The offer is either sent from their mobile operator or a third party. The core of the service is the tracking of user location, used by the mobile operator to send relevant offers. In the first service, the offers are only based on location. In the second service, the offers are based on location and interest, and in addition to location, the mobile operator must gather browsing history. The third service is identical to the second with respect to the data collected. However, in the third service, the data is shared with the stores the consumer visits, and the stores can send them offers. Table 1 presents the two factors used in the design, data sharing, and discount. We presented the respondents with one data-sharing service at a time (the within factor), all with either a discount or not (the between factor).

2.2. Samples and control variables

The respondents were drawn from online survey panels in Norway, Serbia, and Malaysia, while in Pakistan a combination of phone and face-to-face interviews were used. The sample was limited to 16–35-year-olds that use the Internet on their mobile phones.[3] Table 2 presents the sample demographics for the total sample and the four-country subsamples. We observe a skewness toward the older half of surveyd age span, with just 40% of respondents being between 16 and 25 years old. This skewness is especially prominent in Norway and Malaysia. Similarly, Serbia and Malaysia have a skewed gender balance, with more women responding than men. Accordingly, we include Gender and Age as control variables in our estimations to reduce the potential effects arising from the skewed samples on the outcome variable.

As described in the introduction, privacy concerns, privacy knowledge, and trust in mobile operators are frequently included in

[3] For this age group in Norway, Serbia, and Malaysia, the population shares using the Internet on their mobile are more than 90%; in Pakistan, 35% (Telenor internal data).

Table 1
Factors in the design: Data sharing and discounts.

Factor and Level	Description
Factor 1: Data sharing	A within-sample factor with three levels
Service 1: Share location with the mobile operator	Consider a situation where you can receive offers via SMS from stores when you pass or visit them. The offers will be sent from your mobile operator. To receive this service, you must let your mobile operator track your current location. The mobile operator will not share your location data with any third parties. The number of SMSs is limited to 10 a month.
Service 2: Share location and browsing history with the mobile operator	Consider a situation where you can receive offers tailored to your interest via SMS from stores when you pass or visit them. The offers will be sent from your mobile operator. To receive this service, you must let your mobile operator track your current location and your Internet browsing history. The mobile operator will not share your location and browsing data with any third parties. The number of SMSs is limited to 10 a month.
Service 3: Share location and browsing history with the mobile operator, which then shares it with a third party	Consider a situation where regardless of where you are, you can receive offers tailored to your interest via SMS from stores you visit often. The offers will be sent from the relevant stores. To receive this service, you must let your mobile operator track your location history and your Internet browsing history and *share* it with the stores you visit. The number of SMSs is limited to 10 a month.
Factor 2: Discount	A between-sample factor with two levels
0% discount	You receive no discount on your mobile service
10% discount	You receive a 10% discount on your mobile service

Table 2
Sample demographics and background attitudes on privacy and trust.

Demographics	Total		Norway		Serbia		Malaysia		Pakistan	
	N	%	N	%	N	%	N	%	N	%
Sample	3244		838		777		856		782	
Male	1442	44.5	446	53.2	267	34.5	340	40.0	389	49.7
Female	1802	55.5	392	46.8	506	65.5	511	60.0	393	50.3
Age										
16–20 years	528	16.3	103	12.3	141	18.3	90	10.6	194	24.8
21–25 years	751	23.2	206	24.6	152	38.0	193	19.7	200	25.6
26–30 years	1051	32.5	315	37.6	262	34.0	282	33.3	192	24.6
31–35 years	980	28.0	214	25.5	216	28.0	282	33.3	196	25.0
Standardized attitudes	Mean	Std. dev.	Mean	Std. dev.	Mean	Std. dev.	Mean	Std. dev.	Mean	Std. dev.
Trust in mobile operator	0.00	1.00	0.04	0.96	−0.17	0.98	−0.41	0.86	0.56	0.93
Privacy concern	0.00	1.00	0.11	1.04	0.22	0.98	−0.13	0.91	−0.20	1.00
Privacy knowledge	0.00	1.00	0.80	0.94	0.22	0.96	−0.36	0.76	−0.68	0.59

studies of consumer behavior. Because these factors could affect the willingness of consumers to use a personalized ad service, we include them in our analysis as controls. We standardize these three variables to have a mean of zero and a standard deviation of one using the total sample.

The lower panel of Table 2 presents the means and standard deviations for these three variables for each country. Positive mean values for trust, concern, and knowledge indicate that for that country, the respondents have greater trust in their mobile operators, more concern about privacy, and better knowledge about privacy than the average respondent in the four-country sample. As shown, there are considerable differences between respondents in the four countries sampled, especially concerning privacy knowledge, which is much higher in Norway, slightly higher in Serbia and lower in Malaysia and Pakistan. For more details on these measures, see the appendix.

Table 3 presents balance tests for the randomization into price discount treatment groups in each of the four countries. The treatment variable is a categorical variable with two levels. We employ a Kruskal–Wallis equality-of-populations rank test for Age, with p-values ranging from 0.10 to 0.65, and a Chi-square test for Gender with p-values ranging from 0.10 to 0.74. Gender is a categorical variable with two levels, while Age is an interval variable that is close to uniformly distributed with no tails. The test results indicate that the demographic variables are well balanced across the two treatments in all four countries.

2.3. Behavioral predictions

There is extensive economic literature on sharing personal information, but according to Acquisti et al. (2016), it is challenging to locate a unifying economic theory of privacy. Consequently, we base our behavioral predictions on the assumptions that (1) consumers value privacy, (2) consumers are willing to make tradeoffs between privacy and money, (3) privacy is a continuous measure (i.e., privacy comes in degrees, and not only have or have not), and (4) the number of actors receiving the information affects the level of

Table 3
Balance test for the variables Age and Gender to confirm randomization.

Country	Variable	Mean with discount	Mean without discount	*p*-value[b]
Norway	Age	27.10	26.51	0.10
Norway	Gender[a]	1.44	1.50	0.10
Serbia	Age	26.53	26.66	0.65
Serbia	Gender	1.63	1.68	0.15
Malaysia	Age	28.00	27.80	0.49
Malaysia	Gender	1.59	1.61	0.74
Pakistan	Age	25.96	25.73	0.58
Pakistan	Gender	1.53	1.47	0.15

[a] Male = 1, Female = 2.
[b] Kruskal–Wallis equality-of-populations rank test for Age and Chi-square test for Gender.

privacy.

Our experiment allows us to study stated preferences along three dimensions of privacy: (1) the amount of personal data shared – the scale effect, (2) resharing of personal data with other commercial actors – the scope effect, and (3) economic incentives to share personal data. For these three dimensions, we formulate three behavioral predictions.

2.3.1. The amount of personal data shared

Assuming that privacy has a value to consumers and is not dichotomous, we expect consumers to prefer to share as little as possible about themselves with commercial actors: we expect a negative scale effect on the willingness to share. We formulate the following hypothesis:

Hypothesis 1. The willingness of consumers to share personal data will decrease when asked to share browsing history along with the location.

2.3.2. Resharing personal data with other commercial actors

Assuming that the number of recipients of personal data affects consumer privacy, we expect consumers to prefer to share their data with as few others as possible: we expect a negative scope effect on the willingness to share. We formulate the following hypothesis:

Hypothesis 2. The willingness of consumers to share personal data will decrease when asked to share data with retailers in addition to the mobile operator.

2.3.3. Economic incentives

Assuming that consumers are willing to trade privacy for money, we expect consumers to be more inclined to share personal data if they are economically compensated. In our case, the benefit is relevant offers, while for half the sample, an extra economic benefit arises from the 10% discount on the mobile subscription. We formulate the following hypothesis:

Hypothesis 3. The willingness of consumers to share personal data will increase if the sharing is connected to a discount on the mobile subscription.

2.4. Cross-country variation

Along with the three dimensions in the behavioral predictions, we also include cross-country dimensions. The four countries (Norway, Serbia, Malaysia, and Pakistan) differ in many economic and social respects, as illustrated by the United Nations' Human Development Index and the Telecommunication Infrastructure Index. For the United Nations' Human Development Index, the four countries range from the top to the lowest quartile. For example, in 2017 Norway ranked 1 of 189 countries included in the index, Malaysia ranked 57, Serbia ranked 67, and Pakistan ranked 150 (United Nations Development Program, 2018). A similar picture emerges with the Telecommunication Infrastructure Index (United Nations, 2020), which combines mobile and fixed subscriptions and Internet usage. Here, Norway scored 0.90, Malaysia 0.76, Serbia 0.62, and Pakistan 0.24 on a scale from 1 to 0. However, as these are country-level variables, we do not use them in our statistical analysis. Instead, these differences represent an essential background when discussing the differences between the countries in our findings.

3. Results

This section presents the mean scores for responses to the likelihood of use questions and the estimation results for the likelihood of use of the services when regressed against discounts, demographics, and attitudes as independent variables. We also evaluate the three behavioral predictions and explore any differences by country.

3.1. The average likelihood of using the ad services

Fig. 1 depicts the average likelihood of using the ad service requiring personal data. We can see a pattern where the participants, on average, are most favorable to Service 1, which only requires sharing location data with the mobile operator. They are slightly less favorable to Service 2, which requires sharing both location data and browsing history with the mobile operator, and least favorable to Service 3, which requires the sharing location history and the browsing history with both the mobile operator and a third party. We can also see that the participants offered a 10% discount on their mobile subscription if they signed up for the services are on average more favorable to the services than the other respondents.

We further note that the likelihood of using the ad services differs between countries, with Norwegians on average being least interested, followed by respondents in Serbia, Malaysia, and Pakistan. To test the significance of the differences between countries in Fig. 1, we use random effect ordered logit models with the countries serving as the explanatory variable. We separately estimate the model for respondents without a discount and then for respondents with a discount. Wald tests of the coefficients for all combinations of countries indicate that these differences are all statistically significant, with all p-values below 0.020.[4] Summing the main country difference from Fig. 1, we can see that Norwegians are less likely than respondents in the other countries to use the services offered both with and without discounts, while Pakistanis are more likely than the respondents in the other countries to use the services if given a discount.

Looking at the results from another perspective, respondents who are unlikely to use the service provide interesting information about the heterogeneity across the sample and between countries. For example, when Service 1 the least data-greedy service, is connected to a discount, this service is the most positively viewed in all four countries. However, 64% of Norwegians, 40% of Serbians, 31% of Malaysians, and 17% of Pakistanis declare that it is unlikely or very unlikely that they will use the service on our five-point scale. This suggests that there are significant differences in attitudes toward using such services within each country, and therefore that their consumer populations are highly heterogeneous. We also observe substantial differences between countries.

3.2. Ordered logit estimation to test behavioral predictions

Table 4 presents the random effect ordered logit estimations for the four countries separately. As discussed, the choice of model is based on the ordinal nature of the survey question and that the respondents each answered three likelihood questions, one for each service. It is important to note that it is not possible validly to compare the estimates of the ordered logit parameters between estimations. We use Stata 16 for all estimations. Service 2 serves as the base scenario in all estimations because this allows us to test Hypotheses 1 and 2 directly. A final qualification is that the measurement of our dependent variable (how likely it is that the respondent would use the service) is on an ordinal scale. Therefore, we are unable to consider the magnitudes of the coefficient estimates, only their direction and significance.

In what follows, we consider the results presented in Table 4 with respect to the behavioral predictions made in Section 2.3, looking especially at the differences between the likelihood of using the different services and the effect of the discount.

3.2.1. The amount of personal data shared

We compare Services 1 and 2 to evaluate the scale effect, how the likelihood of using a personalized ad service changes when the service demands more personal data. From Table 4, we can see that the primary trend is that the willingness to use the ad service decreases with the level of data the users must share. In three of the four countries, Norway, Malaysia, and Pakistan, the respondents are significantly less likely to use Service 2 than Service 1 ($p < 0.05$). The difference is that Service 2 requires sharing both location and browsing history, whereas Service 1 only requests location. In Serbia, there is no significant difference in the likelihood of use between the services.

Overall, the results in Norway, Malaysia, and Pakistan are in line with Hypothesis 1. They show that the willingness to share personal data decreases when consumers need to share more personal data in most countries. Nonetheless, even with the critical differences between only location data and when combining location and browsing data, the shift in responses from Service 1 to Service 2 is small (as illustrated in Fig. 1).

3.2.2. Resharing personal data with other commercial actors

To test the scope effect, how the likelihood of using the ad service is affected when the number of actors that can access the personal data increases, we compare Services 2 and 3. The respondents are significantly more likely to use Service 2, where location and browsing history are only shared with the mobile operator, than Service 3, where the data are shared with other commercial actors in the two European countries Norway and Serbia ($p < 0.01$). In Malaysia and Pakistan, we do not observe a significant change.

The results in Norway and Serbia correspond to Hypothesis 2. They show that, at least in the European countires in our study, the willingness to share personal data decreases when the mobile operator shares the data with retailers. Once again, as illustrated in Fig. 1, even though the results are statistically significant, they are small in an economic sense when we move from sharing information with the mobile operator alone to including third parties.

[4] $W_{NO\text{-}SE\ no\ disc} = 99.52$, $p = 0.00$; $W_{NO\text{-}SE\ disc} = 89.76$, $p = 0.00$; $W_{NO\text{-}MA\ no\ disc} = 247.80$, $p = 0.00$; $W_{NO\text{-}MA\ disc} = 182.09$, $p = 0.00$; $W_{NO\text{-}PA\ no\ disc} = 142.73$, $p = 0.00$; $W_{NO\text{-}PA\ disc} = 533.63$, $p = 0.00$; $W_{SE\text{-}MA\ no\ disc} = 33.14$, $p = 0.00$, $W_{SE\text{-}MA\ disc} = 17.52$; $W_{SE\text{-}PA\ no\ disc} = 5.40$, $p = 0.02$; $W_{SE\text{-}PA\ disc} = 222.36$, $p = 0.00$; $W_{MA\text{-}PA\ no\ disc} = 10.19$, $p = 0.00$; $W_{MA\text{-}PA\ disc} = 122.91$, $p = 0.00$

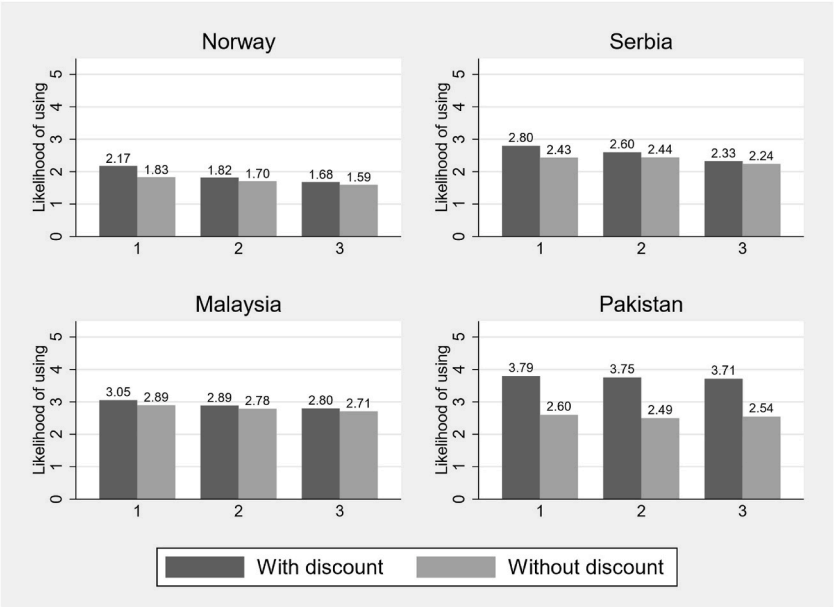


Fig. 1. Mean stated likelihood of use for each ad service. *Note: Likelihood of use is measured on a* five-point scale from 1 = very unlikely to 5 = very likely.

Table 4
Likelihood of using the ad service—random effects ordered logit estimation.

Independent variables	Norway	Serbia	Malaysia	Pakistan
Service 1	0.58***	0.02	0.34*	0.43*
	(3.45)	(0.11)	(2.50)	(2.46)
Service 3	−0.52**	−0.58***	−0.24	0.13
	(–2.93)	(–3.71)	(–1.78)	(0.77)
Discount and Service 1	1.25***	1.01***	0.42	4.72***
	(4.73)	(3.60)	(1.83)	(12.38)
Discount and Service 2	0.68*	0.42	0.33	4.95***
	(2.52)	(1.50)	(1.45)	(12.89)
Discount and Service 3	0.60*	0.22	0.25	4.65***
	(2.14)	(0.78)	(1.07)	(12.21)
Age	−0.03	−0.05*	0.07***	−0.04
	(–1.39)	(–2.37)	(3.54)	(–1.41)
Female	0.06	−0.43	−0.56**	2.82***
	(0.27)	(–1.63)	(–2.75)	(8.39)
Level of concern	−1.02***	−0.90***	−0.72***	−0.42*
	(–8.32)	(–6.48)	(–6.06)	(–2.54)
Level of knowledge	−0.78***	−0.41**	−0.92***	−0.35
	(–5.64)	(–2.78)	(–6.27)	(–1.23)
Trust in mobile operator	0.39**	0.46***	0.87***	0.57**
	(3.04)	(3.41)	(7.08)	(3.19)
N (three responses per respondent)	2401	2216	2426	2334

Notes: *t*-statistics in parentheses; $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$.

3.2.3. *Economic incentives*

In general, the participants presented with offers including a 10% discount on their mobile subscription were more favorable toward the ad services than those without a discount. The effect of the discount is by far the most substantial in Pakistan ($p < 0.001$ for all three services). There is also a significant increase in the likelihood of use for all three services when offering a discount in Norway ($p < 0.05$). However, in Serbia the change with a discount is only significant for Service 1 ($p < 0.001$) and in Malaysia for non. All estimated parameters related to the discount, both significant and not, display their expected positive sign.

These results mostly support Hypothesis 3 and show that consumers in 3 of 4 countries are more willing to use an ad service that requires sharing personal data if given an economic benefit in the form of a discount on their mobile subscription. Hence, respondents are on average willing to make a tradeoff between personal data and money. However, as illustrated in Fig. 1, the differences are small in most countries except Pakistan.

For Norway and Serbia, we see that the effect of the 10% discount decreases as the services become more personal-data intensive. Typically, the discount effect is stronger for Service 1 than Service 2. This result is consistent with consumers evaluating the tradeoff between benefits and cost. The higher the cost in the form of sharing personal data, the smaller the number of respondents that find that a 10% discount is sufficient. Hence, for more personal-data-intensive services, the discount must be higher for as many to sign up for the service as the less data-demanding services. Again, Pakistan differs from the other countries where the 10% discount has approximately the same effect on all services.

3.2.4. *Cross-country differences relating to concern, knowledge, and trust*

We observe the most prominent differences between countries for *privacy knowledge*, with Norway 1.48 standard deviations above Pakistan, with Serbia and Malaysia in between (Table 2). Increasing levels of knowledge then result in significantly lower likelihoods of using a service in all countries except Pakistan, where the level of knowledge is deficient (Table 4).

There are also considerable differences in *trust in mobile operators* across countries (Table 2). Pakistan, which scores lowest on privacy knowledge, scores highest on trust in mobile operators. Malaysia scores lowest on trust, almost one standard deviation below Pakistan. For all four countries, we observe a positive relationship between trust in mobile operators and the likelihood that the respondents will use the services (Table 4).

For *privacy concern*, the two European countries score highest and the two Asian countries lowest, but the differences are minor compared with those for knowledge and trust (Table 2). For all four countries, we observe a negative relationship between privacy concern and the likelihood that respondents will use the services (Table 4).

4. Discussion and conclusion

This paper considered factors that affect consumers' willingness to share personal data with a commercial actor to obtain a personalized offer in Norway, Serbia, Malaysia, and Pakistan. Technological developments over the last decade have given consumers access to the Internet everywhere, facilitating access to fast data networks, smartphones, and social media. As a result, many commercial transactions in developed and developing countries now include transferring personal data from consumers to firms.

We find evidence that mobile Internet users aged 16–35 years care about their privacy when they encounter commercial actors. Many make tradeoffs in terms of how much data they are willing to share and with whom. Our survey results indicate that the willingness to share data decreases with the amount of data and the number of commercial actors that receive the data. The willingness to share also decreases with consumers' privacy concerns and privacy knowledge and increases with their trust in mobile operators. Furthermore, we find that small economic incentives increase the number of consumers willing to give up their data, especially in less wealthy countries. The results are in line with the findings in the privacy literature (Acquisti et al., 2020) and extend it by analyzing privacy in a mobile setting with location data and across a diverse set of countries.

By going beyond the typical WEIRD samples used in most digital privacy studies (Acquisti et al., 2020), this article provides new insights from non-WEIRD countries and the possibility of comparing WEIRD and non-WEIRD countries. While there are many similar preference patterns in the four countries studied, significant differences also require further attention. Our findings indicate that privacy insight generated in a WEIRD context is not necessarily valid outside that context.

The country differences are in line with expectations based on the economic and technological development of the four countries, as seen in the United Nations' Human Development Index and the Telecommunication Infrastructure Index. Norway is one of the world's wealthiest and most technologically developed countries, and few respondents were interested in the personalized ad service. Even with a 10% discount on their mobile subscriptions, less than 20% of young Norwegians were interested in the service.

In contrast, for Serbia and Malaysia, both middle-income countries, the share interested in the service was higher than in Norway, both with and without a discount. In these two middle-income countries in Europe and Asia, adding the discount on the mobile subscription resulted in about a third of young respondents being interested in the service. The poorest and least technologically developed of the four countries, Pakistan has the highest share interested in the service both with and without the discount. Three out of every four young Pakistani respondents were interested in the least data-greedy service with the discount. This suggests that consumers in developing countries are more likely to give up personal data to receive personalized offers. Adding a discount to the subscription strengthens this tendency.

Businesses that want to provide personalized services need to build trust with their customers, find a balance between well-targeted services and customers' personal space, and consider the economic benefits for the customers. Table 4 shows that those consumers who trust their mobile operators are more willing to use the ads service and share their data with the mobile operator. Less data-hungry services are met with a higher willingness to use than those demanding more personal data. Providing consumers with economic incentives increases the number of consumers willing to use the personalized services. Businesses using personal data as part of their business model need to know their customers' preferences in their context to ensure that they strike the best balance.

Our study fills a gap in the literature on privacy in non-WEIRD countries. However, the data is from 2017 and the personal data ecosystem is continuously developing, with new technology, market offerings, and regulations. One example of change is the strengthening of regulations of personal data in several developed countries in the last few years. The introduction of the EU's General Data Protection Regulation (GDPR) in 2018 affected our WEIRD country Norway. It is worth noting that people's attitudes may change slower than regulations and that the rapid development in digitalization and e-commerce have not reached all countries. A study by Wasenden (2020) of privacy concern and knowledge in Norway using data collected before and after the introduction of GDPR and the so-called Cambridge Analytica scandal (Isaak & Hanna, 2018), find only a minor change in privacy concern, while the change in privacy knowledge is more significant. The results from Wasenden (2020) move Norway, the WEIRD country in our study, further up

the ladder on privacy knowledge. For Pakistan, the least economically and technologically developed country in our study, recent articles by Jamil (2021) and Imtiaz et al. (2020) describe a slow digitalization and development in e-commerce, respectively. We find differences between the four countries, following the patterns of socio-economic and technology development. An interesting question for further research is whether privacy attitudes follow socio-economic and technology development over time.

Because of the complexity of digital privacy, individuals struggle to handle privacy issues, and there is a need for policy intervention and regulations in the form introduced by the European Union and Japan. Our analysis points toward another policy area that need attention — education. In our study, the level of knowledge on digital privacy issues is deficient in a large share of the population, and knowledge is negatively correlated with the likelihood of using the personalized service. Given the complexity of online data protection and the pace of digitalization, public and private actors should consider educational measures on digital privacy in all age groups.

Declaration of competing interest

None.

Data availability

The authors do not have permission to share data.

Appendix 1

Our analysis includes three knowledge and attitude measures: privacy knowledge, privacy concern, and trust in mobile operators. The instruments for privacy concern and privacy knowledge are mainly based on Kobsa et al. (2016), Trepte et al. (2015), and Park and Jang (2014). See Evjemo et al. (2020) based on the same data for more discussion on privacy knowledge, privacy concern, and trust in mobile operators in our context. Compared with Evjemo et al. (2020), we have re-estimated and standardized the variables for easy interpretation and comparison in our analysis.

Table 5 presents the five items used as instruments for privacy concern. The items use a five-level scale going from "strongly agree" to "strongly disagree." A confirmatory factor analysis gives a Cronbach's alpha of 0.84, indicating that the items have a high degree of correlation. The privacy concern instrument is constructed using the Stata procedure for constructing latent variables and after that standardized across the whole sample to have a mean of zero and standard deviation of one.

Table 5
Items in privacy concern instrument.

Statements to measure privacy concern
I am concerned that online companies are collecting too much personal information about me
It bothers me when I cannot control how my personal information is used by online companies
It usually bothers me when mobile applications ask me for personal information
I believe that mobile applications ask for more data than is needed to fulfill the purpose of the app
It bothers me that personal information given to online companies for a specific purpose can be used for other purposes

Table 6 present the nine items used in the privacy knowledge instrument. They are measured through a five-point scale from "definitely true" to "definitely wrong." A confirmatory factor analysis of the items results in a Cronbach's alpha of 0.75, indicating that the items have an acceptable degree of correlation. The privacy knowledge instrument is constructed by taking the sum of the nine items before standardized across the whole sample to a mean of zero and a standard deviation of one.

Table 6
Items in privacy knowledge instrument.

Knowledge statements
Facebook, Google, and similar companies track your activity on the Internet
Many mobile apps record your location
Social network site operators such as Facebook also collect information about nonusers of the social network site
When a mobile app has a privacy policy it means that no personal data are shared with other apps or companies
Facebook, Google, and similar companies delete personal data after a predefined period
App providers only collect personal information that is needed to deliver the service
When you deactivate GPS on your phone, your location cannot be tracked
Your browsing history is normally stored on your mobile phone
It is not possible to hack into private information on a mobile phone

We measure trust in mobile operators through one item "My mobile operator is trustworthy" with a five-point scale from "strongly

agree" to "strongly disagree." Like the other two variables, this is also standardized across the whole sample with a mean of zero and a standard deviation of one.

References

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

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology, 30*(4), 736–758.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26–53.

Benndorf, V., & Normann, H. T. (2018). The willingness to sell personal data. *The Scandinavian Journal of Economics, 120*(4), 1260–1278.

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

Brown, M., & Muchira, R. (2004). Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research, 5*(1), 62–70.

Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., Haddadi, H., & McAuley, D. (2015). Personal data: Thinking inside the box. *Aarhus Series on Human Centered Computing, 1*(1), 4.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology Management, 6*(2), 181–202.

Chen, P. T., & Hsieh, H. P. (2012). Personalized mobile advertising: Its key attributes, trends, and social impact. *Technological Forecasting and Social Change, 79*(3), 543–557.

De Keyzer, F., Dens, N., & De Pelsmacker, P. (2015). Is this for me? How consumers respond to personalized advertising on social network sites. *Journal of Interactive Advertising, 15*(2), 124–134.

Evjemo, B., Grønnevet, G., Ling, R., Nag, W., Røhr, H. L., & Wasenden, O. C. (2020). Privacy on smartphones. In R. Ling, L. Fortunati, S. S. Lim, G. Goggin, & Y. Li (Eds.), *The Oxford handbook of mobile communication and society* (pp. 563–579). Oxford: Oxford University Press.

Haghirian, P., Madlberger, M., & Inoue, A. (2008). January. Mobile advertising in different stages of development: A cross-country comparison of consumer attitudes. In *Proceedings of the 41st annual Hawaii international conference on system sciences (HICSS 2008) (48-48)*. IEEE.

Imtiaz, S., Ali, S. H., & Kim, D. J. (2020). E-commerce growth in Pakistan: Privacy, security, and trust as potential issues. *Culinary Science & Hospitality Research, 26*(2), 10–18.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer, 51*(8), 56–59.

Jamil, S. (2021). From digital divide to digital inclusion: Challenges for wide-ranging digitalization in Pakistan. *Telecommunications Policy, 45*(8), 102206.

Kobsa, A., Cho, H., & Knijnenburg, B. P. (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors: An elaboration likelihood model approach. *Journal of the Association for Information Science and Technology, 67*(11), 2587–2606.

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

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734.

O'Malley, L., Patterson, M., & Evans, M. (1997). Intimacy or intrusion? The privacy dilemma for relationship marketing in consumer markets. *Journal of Marketing Management, 13*(6), 541–559.

Peppers, D., Rogers, M., & Dorf, B. (1999). Is your company ready for one-to-one marketing. *Harvard Business Review, 77*(1), 151–160.

Rosenthal, S., Wasenden, O. C., Gronnevet, G. A., & Ling, R. (2020). A tripartite model of trust in Facebook: Acceptance of information personalization, privacy concern, and privacy literacy. *Media Psychology, 23*(6), 840–864.

Schudy, S., & Utikal, V. (2017). 'You must not know about me'—on the willingness to share personal data. *Journal of Economic Behavior & Organization, 141*, 1–13.

Schwartz, P. M. (2019). *Global data privacy: The EU way* (Vol. 94, pp. 771–816). New York University Law Review.

Segijn, C. M., Voorveld, H. A., & Vakeel, K. A. (2021). The role of ad sequence and privacy concerns in personalized advertising: An eye-tracking study into synced advertising effects. *Journal of Advertising*, 1–13.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). October. E-Privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on electronic commerce* (pp. 38–47).

Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019). Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 13*(2). Article 1.

Taylor, C. R., & Carlson, L. (2021). The future of advertising research: New directions and research needs. *Journal of Marketing Theory and Practice, 29*(1), 51–62.

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research, 9*(3), 203–223.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law. Law, governance and technology series* (Vol. 20, pp. 333–365). Dordrecht: Springer.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562.

United Nations. (2020). *E-Government Survey 2020 - Digital Government In The Decade Of Action For Sustainable Development*. Retrieved from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf.

United Nations Development Programme. (2018). *Human development indices and indicators*. Retrieved from http://hdr.undp.org/en/content/human-development-indices-indicators-2018-statistical-update.

Varian, H. R. (2010). Computer mediated transactions. *The American Economic Review, 100*(2), 1–10.

Varian, H. R. (2014). Beyond big data. *Business Economics, 49*(1), 27–31.

Wang, Y., Min, Q., & Han, S. (2016). Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence. *Computers in Human Behavior, 56*, 34–44.

Wasenden, O. C. (2020). Digitalt personvern – kunnskap, bekymring og atferd. *Magma*, (2), 64–73.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389–418.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89.