"Fairly truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure

Miguel Malheiros[1], Sören Preibusch[2], and M. Angela Sasse[1]

[1] University College London, Information Security Research Group
Gower Street, WC1E 6BT, London, UK
{m.malheiros,a.sasse}@cs.ucl.ac.ul
[2] Microsoft Research, 21 Station Road, CB1 2FB, Cambridge, UK
spr@microsoft.com

Abstract. While personal data is a source of competitive advantage, businesses should consider the potential reaction of individuals to certain types of data requests. Privacy research has identified some factors that impact privacy perceptions, but these have not yet been linked to actual disclosure behaviour. We describe a field-experiment investigating the effect of different factors on online disclosure behaviour. 2720 US participants were invited to participate in an Amazon Mechanical Turk survey advertised as a marketing study for a credit card company. Participants were asked to disclose several items of personal data. In a follow-up UCL branded survey, a subset (N=1851) of the same participants rated how they perceived the effort, fairness, relevance, and sensitivity of the first phase personal data requests and how truthful their answers had been. Findings show that fairness has a consistent and significant effect on the disclosure and truthfulness of data items such as weekly spending or occupation. Partial support was found for the effect of effort and sensitivity. Privacy researchers are advised to take into account the under-investigated fairness construct in their research. Businesses should focus on non-sensitive data items which are perceived as fair in the context they are collected; otherwise they risk obtaining low-quality or incomplete data from their customers.

Keywords: personal data disclosure; privacy; effort; fairness; relevance; sensitivity

1 Managing Disclosure of Personal Data

Customers' personal data is seen as a source of competitive advantage by businesses in the information society. The low-cost of storage technologies and the increased efficiency with which large quantities of data can be transferred between systems and analysed have removed most economic disincentives for widespread data gathering efforts. At the same time, the potential benefits realisable through the processing of these data, such as better customer targeting, personalised service, or risk management, contribute to create a seemingly very attractive value

proposition for companies. Left out of this equation, however, is the potential negative impact of customers' behaviour when dealing with requests for their personal data that, for some reason, are deemed too unappealing to comply with. Individuals value their personal data and, if they do not consider truthful disclosure advantageous to them, they may engage in privacy protection behaviours such as withdrawal from the data collection interaction or omission or falsification of data. These behaviours can thus represent lost business opportunities or a lowering of the quality of customer data held, both of which constitute adverse economic effects for the business.

When individuals disclose their personal data to an organisation in exchange for some product or service they are engaging in a social contract; while the benefits of this contract are higher then the costs they will continue engaged [1] [3]. Thus, even interactions that pose privacy risks may be accepted by individuals looking to realise a gain bigger than the perceived privacy cost [5]. In particular, several studies have shown that individuals are willing to trade their personal data for economic benefits such as money rewards (e.g.: [6] [8] [9] [10] [12]). If the rewards are not considered worth the cost of disclosure, individuals may engage in privacy protection behaviours by either withholding [13] or falsifying personal data [14] [15]. This can be interpreted as an attempt to minimise the costs of disclosure while still obtaining the reward. However, it is unclear how prevalent privacy protection behaviours are, or what combination of factors trigger them.

Previous privacy research has identified several factors that affect how individuals perceive the collection and use of their personal data.

Sensitivity. Individuals do not see all personal data as equally sensitive. Typically, more personally defining or identifying items, such as social security number [17], financial data [21] or medical data [20] are perceived as more sensitive; however, sensitivity assessments can vary with the situation [4]. Collection, storage, and use of more sensitive items are associated with feelings of discomfort [20] and perceptions of privacy invasion [18] [19]. Consequently, individuals are more likely to omit or falsify [17] [22] data they consider sensitive.

Perceived Relevance. The same data request can seem more or less acceptable, depending on the context where disclosure occurs. Being asked about cases of cancer in the family during a doctor's appointment is considered relevant, but if one was asked the same question when applying for a store's loyalty card it would be considered irrelevant and inappropriate. Relevance of a data request is related to the perceived data needs of the receiver in that context and whether the expected usage of the data is perceived as legitimate [25] [26]. Lower relevance or legitimacy of a data request is associated with a higher privacy cost [23] and feelings of privacy invasion [19] [24]. Lower perceived relevance of a data request has not been associated with privacy protection behaviours.

Perceived Fairness. Perceived fairness of a data requests describes the individual's belief that data being collected will be used for the purpose communicated by the data receiver, and in an ethical manner [3]. Past research has shown that

when individuals believe that their personal data will be processed fairly they perceive data practices in a more positive manner [22]. Beyond privacy, perceived fairness has been associated with customer satisfaction and higher perceived service quality [3]. No research has been done on the effect of perceived fairness of data requests on disclosure behaviour. Horne et al. [16] explored the impact of the perceived difference between the value obtained by an individual and the data receiver and lying and found no effect.

Data Receiver. It is widely accepted that individuals' perceptions of data practices involving their personal details depend on the organisation with whom they are interacting [30]. However, this relationship between comfort with the data practice and organisation is not linear. While individuals usually feel more comfortable disclosing personal data to organisations with whom they have an existing and trusted relationship [20], such as an employer [18] [19], such is not the case when the data portrays the individual in a bad light. Negative data increases sensitivity when shared with close data receivers [4] [27].

Data Usage. The purpose of the data collection and the perceived use that organisation will make of their data affects individuals' privacy perceptions [20] [21]. One of the main concerns refers to secondary data use, where data that was collected in one context and for one purpose is then used to achieve a completely different goal [24] [4]. Another concern is that data is used in a way that harms the individual who disclosed it. The potential negative consequences of a disclosure can make individuals reticent to part with their personal data or make them perceive a data practice as invasive [18] [21] [27].

Effort. In addition to privacy costs there are other costs associated with disclosure, such as the effort involved in answering data requests. If a data request is difficult to answer [23] or a larger number of data items are requested [28] [9], individuals will perceive the interaction as more costly. The higher the perceived effort the more likely an individual is to withhold data [9].

Privacy Protection Behaviours in Web Forms. Previous work has shown that consumers resist to data collection via forms: Among German Web users, 25% state they have entered false data into forms [32], half of whom have faked their name or age. Unease with the amount of data collected is the main driver for users to falsify their information, followed by the attempt to escape unsolicited advertising. Faking is also observed on online social networks, in particular for younger users, although with overall lower prevalence [31]. In a survey among active social media US consumers, 88% indicated to intentionally have left information out or entered incorrect information when creating a new account at a Website—an increase by 12 percentage points compared to the previous year [33].

Contribution. While some of the factors above have been linked to privacy concerns, not all have been linked to actual privacy behaviour. Making the connection to privacy behaviour is important because past research has shown that

stated privacy concern may not correspond to privacy behaviour [29] [22]. Individuals taking part in research often exhibit a social desirability bias when answering questions about personal data collection manifesting higher concerns than what their behaviour suggests. Thus, observation of actual disclosure behaviour in contextualised scenarios is a more reliable indicator than self-reported privacy attitudes. In this paper, we describe an online field-experiment on the impact of perceived effort, fairness, relevance, and sensitivity of a data request on the decision to answer the request and truthfulness of answer. We believe this is the first large-scale experimental study to quantify the impact of four factors on disclosure decision and disclosure truthfulness. We also test the impact of reciprocity, materialism, and privacy concern on amount of data disclosed.

Paper Structure. We outline our experimental hypotheses in Section 2. In Section 3 we describe our 2-phase experimental design and provide reliability statistics for the scales used. We report and discuss our sample composition, item disclosure rates by treatment, and the effect of the different factors on disclosure and truthfulness in Section 4. Section 5 presents our conclusions on the implications of our study for research and practice, limitations of our work, and directions for future research.

2 Experimental Hypotheses

Based on the analysis of past research on privacy perceptions (see Section 1), we hypothesise that some factors related to how individuals perceive data requests will influence the way they chose to respond to them. For our analysis we chose two factors which have been linked to disclosure behaviour: sensitivity and effort; and two which, to our knowledge, have only been linked to privacy attitudes: perceived relevance and fairness. We measure two different variables regarding disclosure: disclosure decision (binary variable) and self-reported truthfulness of answer (4-level scale).

We predict sensitivity and effort will have a negative effect on disclosure and truthfulness and that perceived relevance and fairness will have a positive effect on disclosure and truthfulness:

H1a: Perceived effort of a request for a data item has a negative effect on decision to disclose that item.

H1b: Perceived fairness of a request for a data item has a positive effect on decision to disclose that item.

H1c: Perceived relevance of a request for a data item has a positive effect on decision to disclose that item.

H1d: Perceived sensitivity of a request for a data item has a negative effect on decision to disclose that item.

H2a: Perceived effort of a request for a data item has a negative effect on the truthfulness of the corresponding answer.

H2b: Perceived fairness of a request for a data item has a positive effect on the truthfulness of the corresponding answer.

H2c: Perceived relevance of a request for a data item has a positive effect on the truthfulness of the corresponding answer.

H2d: Perceived sensitivity of a request for a data item has a negative effect on the truthfulness of the corresponding answer.

We further hypothesise that reciprocity and materialism will affect amount of disclosure, but not privacy concern as measured by Westin's index:

H3a: Reciprocal individuals disclose more data than non-reciprocal individuals.

H3b: Individuals more concerned about privacy do not disclose less data than individuals less concerned about privacy.

H3c: More materialistic individuals disclose less data to minimise privacy cost and maximise value of answering.

3 Experiment Methodology

3.1 Phase 1: the Platixx Web form

After pre-testing, 2720 US participants were invited through the crowdsourcing platform Amazon Mechanical Turk (mTurk) in early 2013 to participate in a "short survey [with] fast approval". The term "survey", commonly found on mTurk, was used although the study is indeed an experiment: participants had to disclose items of personal data rather that stating their willingness to do so. The experiment therefore uncovers actual willingness to disclose rather than self-professed preferences.

The experiment design closely follows an earlier study on voluntary data disclosure [34]. A Web form with 5, 10, or 15 questions was given to the participants, depending on treatment. Some of the questions clearly relate to a banking context (e.g., income, debt situation, spending, number of credit cards), others are plausible indicators of social and demographic status (e.g., age, gender, marital status, health, education). Some questions are uncommon in banking context, such as the number of relatives who died during the childhood or the duration of the longest relationship. However, these factors have been found to be potentially good predictors of credit-worthiness [35].

In accordance with the mTurk guidelines, highly sensitive questions or questions asking for identifying personal details were not included. The order of the questions was not randomised but constant; treatments with fewer questions were truncated not to include all the items.

Across all treatments, there were also two extra mandatory check questions (6 and 7) which tested whether participants had read the instructions properly. The mandatoriness of the other questions varied by treatment, with the other 5, 10, or 15 questions being mandatory as well. If there were mandatory questions, these were always at the beginning of the form and any optional ones towards the end. The instructions, displayed at the top of the form, were adjusted accordingly. There was no visual indicator of mandatoriness (such as starring or highlighting) and the blocks of questions were not separated. All questions were answered using free text fields. There was no warning if some mandatory items had been omitted or if the answer did not match the required format (e.g., no input validation for date of birth).

In total, a 3×4 full triangular design with 9 treatments was run, covering all combinations of question count ($X = 5, 10, 15$) and subset cardinality of mandatory items ($Y = 0, 5, 10, 15$)—excluding the check questions from now onwards. Throughout the remainder of the paper, the following short-hand will be used to refer to the different treatments: qXmY, where X is the total number of questions and Y is the number of mandatory questions amongst those.[3]

The Web form was framed as a preparation for the launch of a new credit card product—the Platixx Card. To gauge the potential interest in this new scheme, Platixx would ask participants to complete a one-page online survey. Using a professionally designed logo and colour scheme, all materials, including the Website URL, were prominently branded as Platixx, a fictitious banking provider.

Participants received 20, 40 or 60 US cents for submitting the form in treatments q5, q10 and q15 respectively. This payment acts as a show-up fee and increased linearly in question count. All participants were paid regardless of whether or not they had complied with the instructions or answered the check questions correctly. As stated in the instructions, no extra payments were made for voluntary over-disclosure. Multiple participation was prevented.

[3] For instance, treatment q5m0 said: “Please provide some information about yourself. Questions 6 to 7 are mandatory. All other fields are optional. There is no bonus for this HIT.” whereas treatment q10m10 said: “Please provide some information about yourself. Questions 1 to 12 are mandatory. There is no bonus for this HIT.”.

Fig. 1. Screenshot of the Platixx Web form in phase 1, treatment q15m0.

3.2 Phase 2: the UCL follow-up questionnaire

After submitting their Web form, participants were invited to a follow-up questionnaire to investigate personality traits, demographics and privacy preferences. Checks were in place to make sure that this questionnaire could only be taken by those who had participated in the first phase (Section 3.1). Two days after the initial invitation, one reminder was sent to those who had not yet taken the follow-up. Across all treatments, a 79% of all phase 1 participants also completed the follow-up survey.

The follow-up was soliciting critical feedback regarding phase 1, including participants' admission to have lied on some questions. To avoid participants giving socially desirable answers, there was a break in the administering party: the follow-up questionnaire was branded as a research study by UCL. The colour scheme and logo differed markedly from the first phase. The purpose was to build trust to induce respondents to answer truthfully. Furthermore, participants were assured that their answers would be kept confidential, and not shared with Platixx. This assurance was re-iterated during the questionnaire whenever sensitive demographic details were solicited, including income, age and gender.

For each question participants had been asked in phase 1 they were asked to rate the perceived effort involved in answering (Cronbach's alpha across all items was $\alpha = 0.91$), its fairness ($\alpha = 0.88$), its relevance ($\alpha = 0.84$), and how truthfully they had answered the question ($\alpha = 0.95$). For 36 general items sensitivity ratings (i.e.: level of comfort with disclosure) were collected ($\alpha = 0.84$). Out of these 36 items, 8 closely matched items collected in phase 1 of the study. An average of the perceived sensitivity of these 36 items was used as a measure of privacy concern, with higher sensitivity averages corresponding to higher levels of concern.

Personality traits were investigated using instruments with established reliability. For measuring materialistic values, the validated 18-item Richins-Dawson scale was used [38]. Reliability was good (Cronbach's alpha $\alpha = 0.89$). Reciprocity was measured on a 6-item, 7-point Likert scale [37] ($\alpha = 0.60$). Privacy attitudes were assessed using the 3-item Westin scale [36], which binned participants into three groups ($\alpha = 0.70$). Using the original terminology, 41% were classified as "privacy fundamentalists", 48% as "privacy pragmatists" and 11% as "privacy unconcerned". According to this segmentation, the participants would have been much more concerned about data protection issues than the general public. Owing to its brevity and its prior use in similar studies, the Westin scale was chosen despite its methodological shortcomings.

3.3 Ethical approval

Both phases of this study were granted permission to be conducted after going through the university's ethical review process.

3.4 Data processing and coding

All answers were manually coded by a single skilled rater into three categories: provided, not provided or refusal. Examples of refusals are: "A lady doesn't reveal her age" or simply nonsense text. Additional data coding was done for some input fields, such as date of birth. In the following analysis, only participants who answered both check questions correctly will be included.

4 Results and Discussion

Across all treatments, there are 2360 valid participants, 1851 of whom also completed the follow-up questionnaire. Table 1 summarises the sub-sample sizes for the different treatments. Explicit refusals to answer and omissions were coded together, so that, for each participant, an item was considered either disclosed or not-disclosed. Based on the information provided in the follow-up, the mean age of participants was 30 years (range from 17 to 80). For 1477 participants, both date of birth from the first phase and age from the follow-up were disclosed and were compared. For 1164 participants (78.8%) there was no discrepancy between the two. Mean discrepancy was 3.43 years. 41% of respondents were women, 59% men according to the follow-up. Less than 1% refused to reveal their gender. For 641 participants there was also gender data available from the first phase questionnaire. When comparing the two gender disclosures only 17 participants (2.7%) disclosed different genders in the first phase and follow-up

4.1 Focus on q15 Treatments

As shown in the top half of Table 1, there is an overriding effect of items being mandatory on disclosure rates. While we plan to explore the mandatory vs. optional relationship with disclosure behaviour in a future publication, in this paper we focus on the effect of perceived fairness, relevance, sensitivity, and effort. Our disclosure analysis here is of the q15m0 treatment, where answers to all data requests are optional. We focus on q15m0 as opposed to q5m0 or q10m0 because it offers a wider range of data items to analyse and identify differences. When investigating the effect of the different factors on truthfulness (Section 4.5), we use all q15 treatments as we do not expect mandatory vs. optional to have an overriding effect. When reporting descriptive statistics for the ratings of perceived fairness, relevance, effort, and sensitivity of data items (Section 4.3) we use data from all nine treatments for the same reason.

4.2 Effect of Personality Traits on Disclosure

We regressed the number of items disclosed by participant on their normalised scores for reciprocity and materialism and Westin category (coded as two dummy binary variables: fundamentalist and pragmatist). We found that only reciprocity was a significant predictor ($\beta = 0.175$, $p < 0.05$) of number of items disclosed.

Whether the participant was a fundamentalist ($\beta = 0.014$, n.s.) or pragmatist ($\beta = 0.053$, n.s.), and level of materialism ($\beta = 0.048$, n.s.) were not significant predictors. The overall model fit was $R^2 = 0.042$.

Reciprocity did have a significant and positive effect on disclosure with more reciprocal participants disclosing more data. Since all the data requests were optional and a reward would be offered unconditionally, it is possible more reciprocal participants felt more obliged to disclose data. The absence of effect of Westin category on behaviour was expected, as there is little evidence that this scale is a good predictor of privacy behaviour and attitudes (see, for example, [39]). The data supports both **H3a** and **H3b**. It was expected that participants who scored higher in the materialism scale would be less likely to disclose data to maximise the value of answering the survey (they would have received a full payment even if no personal data was disclosed), but that was not the case. **H3c** was not supported.

We also regressed number of items disclosed on age and gender but found no significant effect of either variable. Finally, we also regressed the same outcome variable on the average perceived sensitivity across 36 items measured on a 5 level scale by itself. We found it to be a significant predictor ($\beta = -3.212$, $p < 0.01$). The overall fit of this model was $R^2 = 0.056$. This finding suggests that gathering perceived sensitivity ratings across a range of personal data items is a better measure of privacy concern and a better predictor of disclosure behaviour than privacy indices such as Westin's.

4.3 Perceived Effort, Fairness, Relevance, and Sensitivity of Data Requests

The bottom half of Table 1 summarises the average perceived effort, fairness, and relavance ratings for all questions across all treatments. All items have negative effort ratings, indicating a perceived low level of effort when answering the questions. Gender, children count, and marital status were considered the easiest questions to answer, which makes intuitive sense since these questions do not seem to imply any calculations or memory effort. Weekly spending, childhood deaths, and monthly income were considered the hardest questions to answer. While weekly spending and childhood deaths do require participants to recall past events and make some calculations, monthly income should, in theory, be easy to recall. It is possible that some participants do not receive their salaries monthly, so have to compute the value to answer the question. In any case, no questions were considered difficult to answer.

Childhood deaths, relationship max length, and good health were perceived as the most unfair questions. The first two, in particular, were perceived quite negatively. One possible explanation is that it may be difficult for participants to understand how these items will be used, and to imagine a fair use of such data. First name, occupation, and monthly income were considered the fairest questions. Both first name and occupation are common questions in surveys. Monthly income is not commonly asked, but possibly due to its also high perceived relevance participant thought it fair to ask in this context.

The items considered most unfair were also the ones considered most irrelevant in the context of a credit card company survey. It seems legitimate to believe participants saw no connection between these questions and the specified purpose of the survey. The items perceived as most relevant were monthly income, debt situation, and credit card count. These are all questions related to financial matters and, therefore, aligned with the context of data collection.

Sensitivity ratings were collected for 36 items, of which 8 closely match items collected in phase 1 of the study. *Annual income* was considered to be an acceptable proxy of *monthly income* and *illnesses* as an acceptable proxy of *good health*.

Unsurprisingly, illness and annual income were considered the most sensitive items. Past research has shown that medical and financial data are usually considered sensitive by individuals. The least sensitive items were gender and education. Both of these questions are commonly asked in surveys for demographics purposes, so it is likely participants are used to them and consider them not sensitive.

4.4 Effect of Fairness, Relevance, Sensitivity, and Effort on Disclosure

The top section of Table 2 shows the models obtained by regressing disclosure of each data item (as a binary variable) on perceived effort, fairness, relevance, and sensitivity (when applicable) of that data item. The models explain between 7% and 20% of the variability in disclosure decision.

Fairness is clearly the most powerful predictor of disclosure decision, with a significant positive effect on the outcome in 11 out of 15 cases, supporting **H1b**. For four data items, fairness has no significant effect: monthly income, health, credit-card count and debt situation. With the exception of health, these are all items with high perceived relevance to the context of credit cards. We suspect fairness may be more important when data requests are considered irrelevant. Perceived fairness of a data request is an under-researched factor in privacy research and has never been linked to disclosure behaviour. Here it emerges as a promising predictor of privacy decision making.

Sensitivity is a significant negative predictor of disclosure for 3 out 8 items: first name, date of birth, and occupation. **H1d** is thus partially supported. The effect of data sensitivity on disclosure decision has been previously observed in the literature [17] [22].

Relevance has a significant effect on the disclosure of 3 data items, but this effect is unexpectedly negative. Similarly, effort coefficients are significant for 3 data items, but positive contrary to out predictions. It is possible that participants who did not answer a question rated it as requiring low effort precisely because they did not answer it. Meanwhile, participants who disclosed the data may have reported a higher effort. Both **H1c** and **H1a** are rejected.

4.5 Effect of Fairness, Relevance, Sensitivity, and Effort on Truthfulness

Truthfulness ratings of each item (a 4-level scale ranging from -2=Completely disagree my answer was truthful to +2=Completely agree my answer was truthful) were regressed on perceived effort, fairness, relevance, and sensitivity (when applicable) of that item. The resulting regression models for each item can be seen in the bottom section of Table 2. The models explain between 10% and 26% of the variability in truthfulness.

Fairness is once again the best predictor, with a significant positive effect on truthfulness on the same 11 items as in the disclosure regressions, supporting **H2b**. Fairness has a particular and significant strong effect in items with low relevance such as relationship max length or childhood deaths, again suggesting that fairness has bigger important when data requests are seen as irrelavant. The truthfulness regressions support the idea that fairness is a strong predictor of privacy decision-making.

Sensitivity is a significant negative predictor of disclosure for 6 items out 8 where it is applicable, supporting **H2d**. Effort coefficients are significant and negative for 2 data items, offering partial support to **H2a**. Taking into account past research, the negative effects of sensitivity and effort (partially supported by the data) were expected [17] [22].

Relevance coefficients are significant in 3 models, but unexpectedly negative in two of them. Only for monthly income truthfulness is the effect positive. Thus, **H2c** is rejected.

treatment	N	N_{valid}	first name	monthly income	good health	date of birth	marital status	occupation	education	times moved	childhood deaths	weekly spending	relationship max length	children count	gender	credit-card count	debt situation
q5m0	300	258	61.6	57.8	74.0	58.1	72.5										
q5m5	300	271	**99.3**	**99.3**	**100.0**	**99.6**	**99.6**										
q10m0	300	262	69.5	60.3	77.1	59.9	76.7	70.2	71.0	69.1	61.8	53.1					
q10m5	300	254	**99.2**	**98.8**	**100.0**	**100.0**	**100.0**	64.6	66.5	62.6	57.9	53.5					
q10m10	300	257	**99.2**	**98.1**	**100.0**	**98.4**	**99.6**	**98.8**	**99.6**	**98.8**	**98.1**	**96.9**					
q15m0	320	279	64.5	64.9	75.3	57.0	74.2	67.0	71.0	67.0	60.2	54.5	61.3	67.4	72.4	65.9	56.6
q15m5	300	253	**99.2**	**98.0**	**99.2**	**98.8**	**99.2**	69.2	70.4	67.2	62.1	51.4	61.3	66.0	67.6	63.2	53.4
q15m10	300	258	**98.4**	**99.2**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**99.6**	**95.0**	71.3	77.5	78.3	76.7	66.7
q15m15	300	268	**97.0**	**98.5**	**100.0**	**99.6**	**100.0**	**99.3**	**99.6**	**99.3**	**99.6**	**95.1**	**93.3**	**99.3**	**98.9**	**97.8**	**95.9**
feedback																	
Effort	mean		−1.47	−0.81	−1.29	−1.27	−1.50	−1.43	−1.49	−1.19	−0.70	−0.56	−1.13	−1.56	−1.65	−1.19	−0.96
	s		0.99	1.29	1.06	1.18	0.91	0.97	0.93	1.17	1.46	1.43	1.26	0.90	0.82	1.23	1.37
Fairness	mean		1.37	1.15	0.29	1.14	1.00	1.22	0.86	0.57	−0.98	0.51	−0.81	0.39	0.91	1.04	0.92
	s		0.93	1.02	1.44	1.09	1.16	0.99	1.23	1.34	1.31	1.35	1.42	1.43	1.35	1.19	1.28
Relevance	mean		0.92	1.35	−0.52	1.09	0.64	1.08	0.39	−0.01	−1.58	0.58	−1.42	0.05	0.44	1.11	1.16
	s		1.35	0.92	1.42	1.14	1.35	1.13	1.41	1.44	0.94	1.39	1.08	1.50	1.55	1.20	1.18
Sensitivity	mean		2.12	2.62	2.70	2.52	1.84	1.98	1.77						1.63		
	s		0.89	0.86	0.97	0.94	0.74	0.78	0.70						0.66		

Table 1. Sample sizes by treatment, as the total number of participants (N) and the number of those who answered the check questions correctly (N_{valid}); amongst the latter, proportions of participants who provided the given data item. Bold numbers indicate that the question was mandatory in this treatment.The lower part of the table gives the feedback descriptives across all treatments (valid cases only) for item effort, fairness, relevance and sensitivity. Effort, fairness, and relevance were measured on a 4-level agreement scale ranging from −2 (strongly disagree that the question was hard, fair, and relevant) to +2 (strongly agree that the question was hard, fair, and relevant). Sensitivity was measured on a 4-level scale ranging from 1 (very happy to disclose) to 4 (very unhappy to disclose). Thus, higher ratings correspond to higher sensitivity. Ratings are only available for a subset of data items; for income and health, happiness to provide annual income and illnesses was asked for, respectively.

Item	R^2	Effort	Fairness	Relevance	Sensitivity	Constant
			item disclosure			
first name	0.174	0.056	0.624^{**}	-0.342^{*}	-0.655^{***}	1.407
monthly income	0.085	0.051	0.063	0.398	−0.193	0.517
good health	0.069	0.188	0.217	−0.132	−0.331	1.736
date of birth	0.206	−0.049	0.586^{*}	−0.304	-0.723^{***}	1.896
marital status	0.101	0.330^{*}	0.388^{*}	−0.032	−0.103	0.510
occupation	0.149	0.129	0.728^{***}	-0.448^{*}	-0.597^{***}	1.326
education	0.125	0.296^{*}	0.484^{**}	−0.173	−0.359	0.789
times moved	0.099	0.022	0.565^{***}	-0.296^{*}	n/a	0.317
childhood deaths	0.153	−0.178	0.685^{***}	−0.312	n/a	0.750
weekly spending	0.108	−0.154	0.381^{*}	0.012	n/a	0.101
relationship max length	0.135	−0.067	0.588^{***}	−0.060	n/a	1.090
children count	0.089	0.175	0.400^{*}	−0.071	n/a	0.403
gender	0.121	0.344^{*}	0.497^{**}	−0.297	−0.329	0.720
credit-card count	0.089	0.027	0.423	0.006	n/a	0.163
debt situation	0.063	−0.047	0.375	−0.028	n/a	−0.008
			item truthfulness			
first name	0.096	0.005	0.384^{**}	-0.189^{*}	-0.355^{***}	1.416
monthly income	0.097	−0.082	−0.082	0.475^{***}	−0.181	0.921
good health	0.096	0.013	0.098	0.124	-0.244^{**}	1.817
date of birth	0.259	−0.032	0.431^{***}	−0.048	-0.613^{***}	1.910
marital status	0.153	0.118	0.361^{***}	0.003	−0.229	1.096
occupation	0.209	−0.034	0.442^{***}	0.077	-0.285^{**}	1.192
education	0.149	0.020	0.339^{***}	−0.010	-0.301^{**}	1.469
times moved	0.188	0.028	0.580^{***}	-0.183^{*}	n/a	0.636
childhood deaths	0.137	-0.146^{*}	0.487^{***}	−0.188	n/a	1.030
weekly spending	0.140	-0.141^{*}	0.285^{*}	0.120	n/a	0.472
relationship max length	0.154	−0.057	0.500^{***}	−0.065	n/a	1.215
children count	0.118	0.032	0.413^{***}	−0.074	n/a	0.885
gender	0.139	0.095	0.307^{***}	−0.013	-0.267^{*}	1.335
credit card count	0.147	−0.050	0.312	0.192	n/a	0.457
debt situation	0.105	−0.032	0.066	0.368^{*}	n/a	0.309

Table 2. Item disclosure (upper part) and item truthfulness rating (lower part) regressed on item perceived effort, fairness, relevance, and sensitivity ratings. Sensitivity is only included in the regression model when applicable to that data item. Nagelkerke's R^2 was used to assess model fit. *significant at $p = 0.05$; **significant at $p = 0.01$; ***significant at $p = 0.005$

5 Conclusions

Detailed personal data from their customers can help companies to gain insights to improve their services, differentiate their products or adapt their pricing regimes. These competitive advantages have to be weighed against consumers' concern for privacy. Previous research has shown that web users are put off by websites asking personal information that they are unwilling to provide. Many web users admit having provided deliberately wrong data on a web form. Conversely, high prevalence of voluntary over-disclosure has been observed in experimental studies with up to 2/3 of online users volunteering sensitive information, such as date of birth. So far, little has been known about the drivers and inhibitors that make users disclose, respectively withhold or falsify personal data on Web forms.

Our large-scale experiment now provides first insights into the determinants of consumers' willingness to disclose personal data on the web. Four factors were hypothesised to influence user behaviour: perceived effort, relevance, fairness and sensitivity. These factors were tested in administering a web form to 2720 web users, who were asked to provide 15 personal details including financial and health information in preparation for the launch of a new credit-card scheme. The visual appearance of the form provided a highly realistic framing. Participants' disclosure behaviour was then contrasted with their judgements of each of the questions on the form, as collected through a follow-up questionnaire.

Unless a field is mandatory, fairness has a significant, consistent positive effect on the disclosure and truthfulness of the response. Fairness is crucial in driving disclosure for all data items, except for those that are obviously relevant for the purpose of the form (in this case of a credit-card scheme: monthly income, health, credit-card count and debt situation). In parallel, there is a significant positive effect of perceived fairness on the truthfulness of the responses. Perceived fairness is particularly influential and very highly significant for seemingly irrelevant data items such as the length of the longest relationship or the number of deaths during one's childhood. No significant support was found for the effect of relevance on disclosure or truthfulness. Perceived effort had a positive effect on disclosure for three items, possibly due to participants who disclosed an item rating it as requiring more effort than the ones who did not. A negative effect of effort on truthfulness was expected, but only found in three items. Partial support was found for the effect of sensitivity: first name, date of birth and occupation disclosure was significantly affected by their sensitivity. For 6 out of 8 data items, lower sensitivity was significantly associated with more truthful answers.

The managerial implications of this experiment are two-fold. First, website operators should capitalise on the positive impact of perceived fairness. If users are convinced it is fair for a web form to ask for certain information, they will be less likely to withhold these details or give false information. This holds regardless of the sensitivity of a data item. Second, past research may overestimated the importance of perceived relevance. A positive effect on disclosure was only observed for a few data items. In parallel, fairness has not received

the attention it deserves in privacy research and offers strong and consistent predictive power of privacy decision-making.

This study opens several new research avenues. In particular, the interplay between optional and mandatory fields in a web form warrants further investigation. It would also be helpful to test the robustness of the results across different contexts. The current study was set in a financial context which is familiar to most consumers. Individuals also have a more or less accurate perception of what information is relevant to the financial industry. Studying disclosure in more hedonistic applications, such as gaming or social networking, would provide a different perspective. Future work should also remedy the limitations of this work. Although mTurk has been found to feature diverse socio-economic backgrounds, users of this platform may be more inclined to volunteer personal data. There may also be a bias from the research-like character of the study, although efforts were made to create a realistic, commercial framing. One way of overcoming these biases may be field observations of user behaviour on popular web forms in the wild.

References

1. Milne, G.R. Gordon, M.E., 1993. Direct Mail Privacy-Efficiency Trade-offs within an Implied Social Contract Framework. Journal of Public Policy Marketing, 12(2), pp.206215.
2. Laufer, R. S., M. Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. Journal of Social Issues, 33(3), pp. 2242.
3. Culnan, M.J. Armstrong, P.K., 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science, 10, pp.104115.
4. Adams, A. Sasse, A., 2001. Privacy in Multimedia Communications: Protecting Users, Not Just Data. In A. Blandford, J. Vanderdonckt, P. Gray, eds. People and Computers XV - Interaction Without Frontiers: Joint Proceedings of HCI 2001 and IHM 2001. London: Springer, pp. 4964.
5. Dinev, T. Hart, P., 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17(1), pp.6180.
6. Hann, I., Hui, K.-L., Lee, S.-Y.T. Png, I.P.L., 2002a. Online information privacy: Measuring the cost-benefit trade-off, in: Proceedings of the Twenty-Third International Conference on Information Systems. L. Applegate, R. D. Galliers, and J. I. DeGross, Barcelona, pp. 110.
7. Hann, I., Hui, K., Lee, T.S. Png, I.P.L., 2002b. The Value of Online Information Privacy: Evidence from the USA and Singapore. International Conference on Information Systems.
8. 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. Alexandria, Virginia, USA, pp. 109118.
9. Hui, K.-L., Teo, H.H. Lee, S.-Y.T., 2007. The Value of Privacy Assurance: An Exploratory Field Experiment. MIS Quarterly, 31(1), pp. 1933.
10. Grossklags, J. Acquisti, A., 2007. When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In Workshop on Economics of Information Security.

11. Kourti, I., 2009. Project FLAME Social Study Report.
12. Beresford, A.R., Kbler, D. Preibusch, S., 2010. Unwillingness to Pay for Privacy: A Field Experiment (No. 5017), Discussion Paper Series. Institute for the Study of Labor (IZA), Bonn, Germany.
13. Sheehan, K.B. Hoy, M.G., 1999. Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. Journal of Advertising, 28(3), pp. 3751.
14. Culnan, M. J. Milne, G.R., 2001. The Culnan-Milne Survey on Consumers Online Privacy Notices.
15. Lwin, M.O. Williams, J.D., 2003. A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online. Marketing Letters 14(4), pp. 257272.
16. Horne, D.R., Norberg, P.A. Ekin, A.C., 2007. Exploring consumer lying in information-based exchanges. Journal of Consumer Marketing 24(2), pp. 90 99.
17. Metzger, M.J., 2007. Communication Privacy Management in Electronic Commerce. Journal of Computer-Mediated Communication, 12(2), pp.335361.
18. Tolchinsky, P.D., McCuddy, M.K., Adams, J., Ganster, D.C., Woodman, R.W. , Fromkin, H.L., 1981. Employee perceptions of invasion of privacy: A field simulation experiment. Journal of Applied Psychology, 66(3), pp. 308313.
19. Woodman, R.W., Ganster, D.C., Adams, J., McCuddy, M.K., Tolchinsky, P.D. Fromkin, H., 1982. A Survey of Employee Perceptions of Information Privacy in Organizations. The Academy of Management Journal, 25(3), pp. 647663.
20. Ackerman, M.S., Cranor, L.F. Reagle, J., 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. In Proceedings of the 1st ACM conference on Electronic commerce. Denver, Colorado, United States: ACM, pp. 18.
21. Phelps, J., Nowak, G. Ferrell, E., 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy Marketing, 19(1), pp. 27-41
22. Malheiros, M., Brostoff, S., Jennett, C. Sasse, M.A., 2012b. Would You Sell Your Mothers Data? Personal Data Disclosure in a Simulated Credit Card Application. Submitted to the 11th Annual Workshop on the Economic of Information Security (WEIS 2012), Berlin, Germany, June 25-26, 2012
23. Annacker, D., Spiekermann, S. Strobel, M., 2001. e-Privacy: Evaluating a New Search Cost in Online Environments. In Proceedings of the 14th Bled Electronic Commerce Conference (BLED 2001). Bled, Slovenia, pp. 292308.
24. Culnan, Mary J. 1993. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. MIS Quarterly 17 (3) (September): 341363. doi:10.2307/249775.
25. Hine C. Eve J., 1998. Privacy in the Marketplace. The Information Society, 14, pp.253262.
26. Malheiros, M., Jennett, C., Patel, S., Brostoff, S. Sasse, M.A., 2012a. Too Close for Comfort: A Study of the Effectiveness and Acceptability of Rich-Media Personalized Advertising. To Be Presented At CHI 2012, Austin, TX, US, May 5-10
27. Malheiros, M., Jennett, C., Seager, W. Sasse, M.A., 2011. Trusting to Learn: Trust and Privacy Issues in Serious Games. In J. M. McCune et al., eds. Trust and Trustworthy Computing. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 116-130.
28. Miltgen, C.L., 2007. Customers privacy concerns and responses toward a request for personal data on the internet: an experimental study (No. 369). Universit Paris Dauphine, DMSP, Paris, France.

29. Spiekermann, S., Grossklags, J., Berendt, B., 2001. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior, in: Proceedings of the 3rd ACM Conference on Electronic Commerce. ACM, Tampa, Florida, USA, pp. 3847.
30. Stone, E.F., Gueutal, H.G., Gardner, D.G. McClure, S., 1983. A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. Journal of Applied Psychology, 68(3), pp. 459468.
31. BITKOM: 12 Millionen Deutsche machen Falschangaben im Web. 2010 http://www.bitkom.org/$62107_6$2102.*aspx*
32. BITKOM: Jedes vierte Mitglied unkert in sozialen Netzwerken. 2011. http://www.bitkom.org/de/presse/$70864_6$7989.*aspx*
33. Janrain. 2011. Research Study: Consumer Perceptions of Online Registration and Social Sign-in. http://janrain.com/blog/research-study-consumer-perceptions-online-registration-and-social-sign/
34. Preibusch, Sren; Krol, Kat; Beresford, Alastair R. 2012. The privacy economics of voluntary over-disclosure in Web forms Eleventh Workshop on the Economics of Information Security (WEIS 2012), 2526 June 2012, Berlin / Germany
35. Hunt, J., Fry, B., 2009. Spendsmart. London: Piatkus Books.
36. Harris and Associates Inc., Westin, A., 1998. E-commerce and privacy: What net users want. Privacy and American Business and Pricewaterhouse Coopers LLP.
37. Gerlitz, J. Schupp, J. 2005. Zur Erhebung der Big-Five-basierten Persnlichkeitsmerkmale im SOEP. Research Notes. DIW Berlin
38. Richins, M. L. Dawson, S. 1992. A Consumer Values Orientation for Materialism and Its Measurement: Scale Development and Validation. Journal of Consumer Research: An Interdisciplinary Quarterly. 19 (3) University of Chicago Press
39. Consolvo, S. et al., 2005. Location disclosure to social relations: why, when, what people want to share. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI 05. New York, NY, USA: ACM, pp. 8190.