JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–10
https://doi.org/10.1093/cybsec/tyad005
Research Paper

Research Paper

Tell me more, tell me more: repeated personal data requests increase disclosure

Piers Fleming [1,*], S. Gareth Edwards [2], Andrew P. Bayliss [1] and Charles R. Seger [1]

[1]School of Psychology, Centre for Behavioural and Economic Social Science, University of East Anglia, Norwich Research Park, Norwich, NR4 7TJ, UK and [2]School of Psychology, University of East Anglia, Norwich Research Park, Norwich, NR4 7TJ, UK

*Correspondence address. School of Psychology, Centre for Behavioural and Economic Social Science, University of East Anglia, Norwich Research Park, Norwich, NR4 7TJ, UK. Tel +44 1603 593386; E-mail: p.fleming@uea.ac.uk

Received 20 July 2022; revised 22 November 2022; accepted 27 February 2023

Abstract

Personal data is of great commercial benefit and potential sensitivity. However, for the consumers who provide their personal data, doing so comes with potential costs, benefits and security risks. Typically, consumers have the option to consent to the use of personal/sensitive data but existing research suggests consumer choices may only be weakly related to their concerns (the privacy paradox). Here, we examine if the repetitive nature of data requests alters behaviour but not concern, therefore, explaining the divergence. This work is theoretically grounded in 'Foot in the door' research in which small initial requests facilitate subsequent larger requests. An initial laboratory study asking for real, personal data demonstrated increased information disclosure at a subsequent request. A second online study replicated the increased information disclosure effect and found no change in associated privacy concern. We find this supports foot-in-the-door as one explanation of the privacy paradox. We suggest ways for businesses and consumers to encourage an acceptable level of disclosure to match personal beliefs for mutual trust and benefit.

Key words: privacy, foot-in-the-door, privacy concern, privacy paradox, personal data

Introduction

Consider the last time you viewed an article from your favourite newspaper website. Perhaps it was this morning. You may have been asked to subscribe (e.g. 'Support the Guardian for as little as £1') or at least turn off your adblocker (e.g. 'Help The Times remain The Times… Please add us to your whitelist'). If you then purchased a book, theatre tickets or an airplane ticket, you were likely asked to complete a 'brief customer survey'—for the second, tenth or hundredth time. You may have read an email asking for a small increase in your monthly donation to the Red Cross. And if you logged into Facebook, it may ask for a little more profile data—your school or workplace for example. Obviously, advertizers, marketers and social media gurus believe that repeated requests will lead to increased compliance. How do these repeated requests change our behaviour, and can they lead us to do things—like sharing personal information—that we otherwise would not want to do?

'The world's most valuable resource is no longer oil, but data' [1]; two of the world's 10 most valuable public companies' businesses are centred around personal data.[1] However, that data comes from individual consumers and, for the individual, loss of control of our personal data can be harmful. There are minor inconveniences such as junk email and more disruptive potential consequences such as identity theft or personal and professional embarrassment following a disclosure or data breach. We are naturally averse to physical and social intrusions to our communications such as eavesdropping [2]. However, despite generally high stated concerns over privacy most people share large amounts of personal information, particularly over social networks, without protecting that information from unintended recipients [3]. There is some variation with some people

1 Specifically, this includes Google's parent company, Alphabet, and Facebook's parent company Meta. Three of the other top 10, Apple, Microsoft and Amazon, also make substantial use of personal data.

being more privacy concerned, but they are in the minority [4]. If we better understand why people share personal data, we can encourage greater sharing when it is mutually beneficial but protect against over-sharing when it might lead to harm or loss of trust.

The phenomenon in which people state considerable privacy concern but do not act to protect their privacy is known as the 'privacy paradox' [5]. Most people state that they are 'moderately or 'very' concerned about privacy but then many admit to revealing personal information for discounts or other minor rewards [6]. Even when the privacy intention and behaviour is matched, consumers disclose more information than their earlier stated willingness to disclose, as measured in a seemingly separate episode [5]. People are willing to divulge personal information to strangers across social networks and to give faceless companies access to highly personal information around major life events. The privacy paradox might be partly because of the complexity and uncertainty around the costs, benefits and consequences of personal data-sharing—which is technologically, legally and logistically complex [7].

In addition to, or because of, the complexity of understanding data-sharing costs and benefits there are also social reasons for personal information disclosures. There is evidence that social identification with a brand leads to greater disclosure [8]. Increasing disclosure by others on a social network increases disclosure, as does similarity to disclosers [9]. Trust, self-presentation and relationship development has also been found to be predictive of self-disclosure, which may be moderated by network size and prestige [10, 11]. Furthermore a range of structural 'nudges' such as cues, warnings, privacy information and defaults can increase or decrease information disclosure, which can be described as 'dark patterns' [12, 13]. This complexity may be a feature of social networks to encourage data sharing.

One feature of computerized privacy requisition is repetition—and this feature may lead to greater personal data-sharing and partly explain the privacy paradox. Often, online database/social network requests initially solicit some information (email/phone/age and so on) and then, via future emails/logins, make subsequent requests for more personal information. For example, upon creating a Facebook profile, the consumer is asked for a variety of information that they would like to share on their profile, such as their current location, hometown and relationship status. If people leave certain areas blank (such as past schooling), they may be prompted to fill these in later. People are further prompted to 'Answer a question to help people get to know you'. Smartphone maps may ask people to track their location and provide reviews of places they have been. Other apps may ask for access a person's browsing history, contacts or other information.

We contend that this pattern of asking for increasing amounts of users' information over time is analogous to a classic compliance technique called the 'Foot in the door' (FITD) effect [14, 15]. In the FITD, a large request (e.g. 'Would you allow our researchers into your home to check what household items you use?' is preceded by a smaller request (e.g. 'Would you answer a few simple questions about household items?'); in this procedure, the second, larger request is much more likely to be successful than without the preceding request. Although the average effect size of the FITD is small, this is a robust and highly replicated finding, i.e. applicable to consumer behaviour and charitable giving [16, 17].

Theoretically, there is some dispute about the cause of the FITD effect, although there is agreement that it is caused by interpretation of the initial response [16, 18]. One theory, self-perception [19], holds that respondents agree to the initial request and then conclude that they are helpful people and this change in attitude makes them more compliant to a subsequent request [20]. However, this process may be more likely in domains such as charitable giving [e.g. 21], than in seemingly mundane interactions with a website. An alternative account is that respondents wish to be internally consistent with their first response [22]. Such consistency motivations may operate outside awareness [23], and have been indicated as one of the primary drivers of human behaviour [24, 25]. The FITD can also work by simply de-sensitizing people to requests on a particular topic. It could be argued the difference between compliance with a small request and a larger, related request is merely one of degree; agreeing to decline or comply with the initial request is where the qualitative difference lies [26]. Similarly, statements and requests are seen as more valid and familiar when they are repeated over time [27, 28].

FITD is a robust phenomenon, which works after delays of days or weeks, for pro-social and anti-social requests, and for low legitimacy requestors such as a special-interest group [16, 29, 30]. While many studies demonstrating FITD make requests in person and may be partially reliant on experimenter effects [16], there have also been demonstrations relayed by computer, e.g. a prior petition elicited 4.9% of visitors to donate compared to 1.6% of visitors who did not receive a petition first [31]. Similarly, it has been found that the FITD was successful in getting people to complete surveys advertized via unsolicited email and conducted over the internet [32].

There is a reason, therefore, to predict that the FITD will be effective in an online setting when focused on the case of personal information disclosure. However, we do not necessarily expect such an approach to alter self-perceptions related to privacy concern. Past research has shown that the FITD can be effective without changing self-perceived altruism [33] or helpfulness [34], and above we have discussed theoretical explanations for the FITD that do not rely on self-perception theory. It may also be the case that self-schemas are less salient when people are asked for information on a website than when they are asked for a charitable donation in real-life (the scenario underlying much FITD research). Should privacy concern remain unchanged in the face of a significant FITD effect, it suggests an origin for the privacy paradox: repeated questioning can change an individual's disclosure behaviour but not his or her attitude towards personal information.

There are alternative inter-related accounts for the potential efficacy of repeated requests for information. It may be that repeated identical requests facilitate a subsequent request by repetition alone, rather than a small request facilitating a large request characteristic of FITD. We know that repeated exposure enhances the credibility of statements [35]. Repetition may normalize an information request, or may affect persuasiveness by greater scrutiny or fatigue with further repetition [36]. Of particular relevance for digital privacy requests is the idea of privacy fatigue or digital resignation [37, 38]. Privacy fatigue has been compared to burnout in which people become exhausted and cynical with regard to privacy over an extended period of being unable to control their personal information and therefore disengage from privacy maintenance. The level of measured privacy fatigue can be more predictive of personal information disclosure than privacy concern [37]. Digital resignation addresses the related idea that accepting the futility of protecting privacy from powerful corporate entities is a rational response [38]. However, while it is important to be aware of the context of research in this area our study focuses on a shorter timescale and only two requests for information which are under participants' control. We believe this design would be insufficient to create fatigue or resignation effects.

Some people may be more susceptible to the privacy paradox than others. What individual differences might determine how people respond to repeated requests for disclosure information? Agreeableness is the extent to which people are favourably disposed to others and is associated with concessions in social situations [39]. Therefore, we might expect greater agreeableness to be associated with greater willingness to disclose [40], thereby linking agreeableness and the FITD effect. It is notable that there is evidence of greater privacy concern with greater agreeableness, which can be attributed to shared responsibility around privacy [41], this may make inferences on the relationship between 'agreeableness' and the privacy paradox more complex.

Social desirability—the willingness to conform with social norms or present oneself in a positive light—may also provide interesting insights regarding the privacy paradox. The FITD effect may rely on people doing the pro-social behaviour of agreeing to the first request, but higher social desirability has also been shown to reduce disclosure of private, sensitive information [42]. Social desirability is, therefore, an ideal individual differences variable with which to investigate personal data sharing.

Two studies investigated repeated requests for personal data, as well as examining the key individual differences measures identified above. An initial laboratory study with incentivized requests for real data found greater willingness to disclose at the second time of asking. A second study used the same methodology but with hypothetical requests for data and replicated this effect. Personality factors and privacy concern did not explain the disclosure of personal data.

Study 1

Study 1 uses a behavioural laboratory-based measure with realistic consequences. Participants were asked to reveal personal information and then to disclose that information publicly to a website for 2 weeks in exchange for a chance of a reward. The aim was to create an analogous situation to real-life data requests, with realistic incentivized rewards and consequences for disclosure. The decreased psychological distance fostered in a laboratory setting increases engagement and decision concreteness. Incentivized choices are more likely to elicit privacy preferences, which predict their actual privacy choices [43]. This is also analogous to websites or apps that require access to data in order to obtain some reward (e.g. ability to take a quiz or view a humorous message). Prior to the laboratory session, we also measured privacy concern, general self-reported privacy behaviour, a brief five-factor measure of personality and a measure of social desirability.

In this study, we asked participants to make the same decision regarding information disclosure twice. As suggested by FITD research, our primary hypothesis was that that compliance at the second request would be greater, following the preliminary request. Furthermore, we hypothesized social desirability and agreeableness would be associated with willingness to disclose, as both factors are associated with agreeing with others' requests. Agreeableness and social desirability might also be associated with greater influence of the FITD effect i.e. even greater disclosure at the second request. We also measured that and self-reported general privacy behaviour and general privacy concern. However, these may not relate to willingness to disclose, as suggested by the privacy paradox.

One exploratory hypothesis was that lack of control over information might increase subsequent disclosure. To examine this a *control* manipulation informed half the participants that their first information disclosure decision was being discarded and the decision of another was being used instead prior to their second disclosure decision.

Method

Participants

A total of 27 participants, nine men, 17 women, one undeclared ($M = 19.3$ years old, SD $= 1.3$) were recruited from a university participant panel, receiving £4 compensation with the possibility of performance based additional rewards of 2 × £5. Therefore, participants could earn £4, £9 or £14 depending upon their decisions in the experiment.

Materials

Participants were asked to disclose personal information as well as privacy concern, self-reported privacy behaviour and personality measures.

Personal information disclosure index (PIDI)

Participants were asked to complete 67 questions about their personal beliefs and behaviour including height, weight, phone number as well as opinions on immigration, abortion, politics and sexual fantasies. These questions were then re-presented to participants during the study, ordered from least-to-most 'intrusive' (as rated by an independent sample in a prior survey). These questions were sampled from the full 70-item H-PIDI minus two questions on employment and one on important conversations (see the full ordered list in the Appendix). Participants worked their way through the list, item by item, and decided if they would 'sell' each item to the experimenters. Participants were told that this sale would involve any information that the participants agreed to sell being published online on a purpose-made website for a 2-week period.[2] For ethical reasons, this information was not published online and participants were fully debriefed at the end of the study. However, the participants all acknowledged that they had made their decisions in the belief that the information would become public. Once a participant reached an item on the list that they did not wish to sell, the decision sequence ended. The PIDI score was the highest numbered item the participant was willing to sell. Each sold item increased the probability of winning an additional £5. For example, if a participant decided not to sell the first item, the session ended and no items were sold in this sequence, and the PIDI would score 0.

Concern for information privacy scale

Participants were asked to complete a 15-item concern for information privacy scale (CFIP) on a 7-point Likert-type scale from strongly disagree to strongly agree, [44], e.g. 'I'm concerned that companies are collecting too much personal information about me' ($\alpha = 0.91$).

Privacy behaviour scale

Participants also completed a 15-item self-reported privacy behaviour scale based on an existing 12-item scale [45], e.g. 'Do you clear your browser history regularly?' and with an additional three items: 'Do you encrypt your data (e.g. on laptop, phone)? Do you make an effort to ensure your social media privacy settings match your preferences? Do you have multiple social media accounts to

2 Participants were not informed precisely how the information would be presented or whether their name would be included. This ambiguity is analogous to real-world situations and supported an ethical but convincing design.

Table 1: Means, standard deviations and zero-order Spearman's *rho* correlations for measured variables

Scale (min–max)	*M*	SD	1	2	3	4
1. Intrusion questions answered pre-test (0–67)	55.7	12.9	–			
2. CFIP pre-test (15–105)	85.2	12.0	−0.08	–		
3. Privacy behaviour pre-test (15–105)	37.2	8.9	0.20	0.51**	–	
4. Personal information disclosure index (items sold 0–67) T1	38.7	20.7	0.42*	0.01	−0.31	
5. Personal information disclosure index (items sold 0–67) T2[4]	43.0	21.3	0.44*	0.04	−0.24	0.90***
6. SDS13 (0–13)	5.7	2.5	−0.17	0.21	−0.13	0.07
7. TIPI—extraversion (2–14)	8.8	2.6	−0.11	0.08	0.02	−0.05
8. TIPI—conscientiousness (2–14)	9.6	2.4	0.09	0.04	0.16	−0.05
9. TIPI—openness (2–14)	10.2	2.2	0.07	0.32	−0.06	0.60***
10. TIPI—agreeableness (2–14)	8.9	2.3	−0.28	−0.15	−0.16	−0.07
11. TIPI—emotional stability (2–14)	9.0	2.7	−0.34	−0.10	−0.27	0.08

Note: * $P < 0.05$, ** $P < 0.01$ and *** $P < 0.001$.

[4]Due to the very high correlation (0.90) between the two PIDI measures, only Time 1 is presented in a column.

compartmentalize your life (e.g. two twitter accounts, one 'professional', one 'private')?' all 15 items were scored on a 5-point scale from never to always ($\alpha = 0.79$).

Personality scales

A 10-item personality inventory was completed [46] as well as a 13-item social desirability scale [47] ($\alpha = 0.57$).

Design

A within subjects design was employed to examine privacy behaviour (Time 1, Time 2). All participants made the same privacy information disclosure index decisions twice, allowing for within-subject comparison. A further between subjects manipulation employed *control* (own, other), which is described below briefly. Measures of individual difference were correlated with PIDI and PIDI change Time 1–Time 2.

Procedure

Participants completed an online questionnaire in which they provided answers to the 67 PIDI questions, presented randomly. Participants then completed the 10-item personality inventory, the social desirability scale, the CFIP scale and the general privacy behaviour scale.

A total of 1–3 days later, participants attended a laboratory session, where they made decisions based on the information they had previously provided online. There were four stages to this part of the experiment:

Stage 1

(T1): the PIDI was re-presented onscreen, one item at a time, ordered from least-to-most 'intrusive' question. Participants decided how much of the previously collected information they were willing to sell (from 0 to 67 items)—they could only choose a question up to which they would sell all of the prior information.

Stage 2:

Participants made the same 'sale' decisions again, but this time they thought that they were deciding whether or not to sell the information of an unknown other participant, with that other participant gaining any rewards associated with the sales. This was included to make the Stage 3 between-subjects manipulation convincing; this data was not analysed.

Stage 3:

At this stage of the experiment, a between subjects manipulation was introduced: half of the participants (the 'other' condition) were informed that their stage 1 judgments would be discarded in place of the sale decisions that an unknown other participant had made on their behalf. The remaining half of the participants (the 'own' condition) existing decisions would be used. The own or other judgement respectively would determine payment from stage 1 and the associated disclosure for the participant.

Stage 4

(T2): all participants completed the same PIDI judgement task as in stage 1, this time for an additional 2-week period of publicity, with the possibility of gaining an additional, separate £5 lump sum.

Results and discussion

As expected, this small-scale experimental study with real incentives found an increase in privacy disclosing behaviour at a second request (see Table 1). Disclosure increased by an average of an additional four-items at second request (mean items sold: T1 = 38.7, T2 = 43.0), $t(26) = 2.44$, $P = 0.022$. There was a substantial range in responses (see Fig. 1). There was no significant difference (or interaction) between the 'own/other' conditions.[3] Thus, our participants would give away more of their own personal information merely having been asked to do so more than once, supporting our primary hypothesis. This behaviour is characteristic of the FITD effect—participants acquiesced to a first request and then were more willing to help at the subsequent request. Indeed, due to the ordering of the sale choices, any additional items would have been more 'intrusive' than those previously sold.

The two PIDI measures were highly correlated with one another as one would expect for the same questions ($r = 0.90$) and were also associated with high openness to experience on the TIPI, but were not associated with privacy concern (CFIP). Privacy concern was associated with general self-reported privacy behaviour and with openness to experience. The reported scores are indicative and uncorrected for multiple comparisons—after Bonferroni correction only the PIDI T1–T2 correlation remains significant. There is little support for our hypothesis that agreeableness and social desirability should lead to increased willingness to disclose.

Non-parametric correlations of the eight self-report measures (CFIP, privacy behaviour, SDS13 and the five TIPI factors) with the PIDI-change between T1 and T2, surprisingly only revealed agreeableness as related ($r(25) = -0.575$, $P = 0.002$). This indicated

3 Sales to other averaged 37.2 (SD = 19.1).

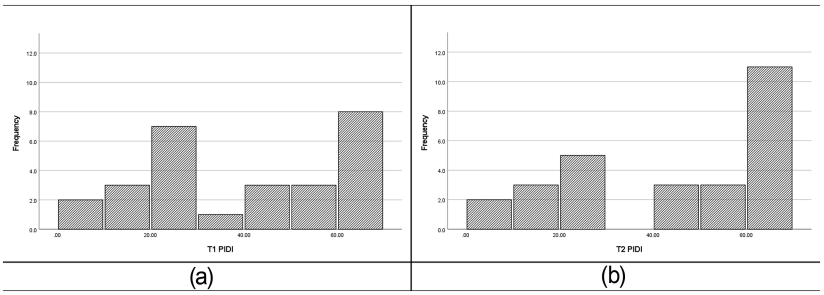

Figure 1: Frequency of PIDI responses at T1 (a) and T2 (b).

that participants low in agreeableness were likely to disclose more at the second time of asking and vice versa. Importantly, our 'ask-twice' effect of increased disclosure on second request was unrelated to 'concern for privacy'. This may speak to the formation of the 'privacy paradox', as here we show that a foot-in-the-door effect acts to change privacy behaviours but does not modulate privacy concern.

We note also that 'privacy behaviour' in general (pre-test) showed a trend for association with general 'privacy concern' but not with the PIDI at T1 or T2. This is important as it suggests that self-report measures of intended or previous behaviours do not match with actual behaviours when it comes to information privacy, in our sample. In general, the privacy disclosing behaviour was also unrelated to the personality measures except a trend for openness to experience being associated with greater self-reported privacy behaviour.

Mean scores for each of the scale variables and zero-order Spearman's rho correlations between them are presented in Table 1. On average, 55.7 intrusive privacy questions were answered in the online pre-test. As expected, participants provided more answers to questions that were (independently rated as being) less intrusive ($r = 0.623$, $P < 0.001$). Further, the more questions a participant answered online, the more information (PIDI) they would 'sell' at both T1 and T2. No other measures related to number of questions initially answered.

We note that although debrief and data analysis did suggest that the privacy disclosures our participants made in the initial online section of this study were genuine, this was not empirically verified. One strategy might be to disclose false information, mitigating any potential negative impact [48]. However, while these limitations may have reduced the power of the study to detect differences they do not explain the greater disclosure at the second request—which supports a FITD account for privacy disclosure.

Overall, there is evidence for a FITD effect for personal information disclosures, which suggests that repeated requests for privacy information (which are common online) will increase disclosure on average. This behaviour was not explained by privacy concern. Further research is needed to address the study limitations and test the robustness of the effect. In order to validate our novel foot-in-the-door finding, and to rule out the potential that our effects result from participant strategies such as providing false information, in Experiment 2, below, we had participants make decisions about hypothetical information. This negates the possibility for negative impacts relating to sharing information, thus removing any motivation to employ a false-disclosure strategy. Finding a foot-in-the-door effect for information sharing under these conditions would provide a stronger base on which to interpret the current findings.

Study 2

Study 2 aims to replicate Study 1 to test whether the effect of repeated disclosure requests is robust. The methodology diverged slightly to support some improvements. First, both privacy concern and disclosure behaviour were measured twice; it may be that as disclosure increases, concern decreases and, therefore, there is no paradoxical gap between behaviour and concern. The measurement was moved online to facilitate a larger sample and more realistic conditions for what is typically an online behaviour. Further, we removed the exploratory between subject manipulation of self/other control, which may have added noise in Study 1.

Potential explanatory variables were added including trust and need for cognition. Trust increases the likelihood of sharing personal information [49] and it follows that people who are generally more trusting might also be generally more compliant. Need for cognition is the extent to which people engage and enjoy evaluation of their environment (NFC) [50]. We would expect those higher in NFC to identify potential risks around personal information disclosure and so reduce it [40], and to reduce the contextual effect of a first request via FITD. Refined measures of social desirability and agreeableness were also used to improve on the short questionnaires that measured these variables in Study 1. The potential problem of false disclosure was removed by using hypothetical disclosure.

In line with Study 1, our primary hypothesis was that disclosure would be greater at the second request but that privacy concern would not change. As secondary hypotheses, we expected need for cognition to decrease privacy disclosure and compliance and trust, agreeableness and social desirability to increase privacy disclosure and compliance.

Method

Participants

A sample of university students were invited to take part in the study for course credit. The final sample consisted of 132 participants; 146 began the survey, two participants withdrew/failed to complete the survey, eight had to be removed due to a technical problem and four were removed for a total completion time under 4 min (under 1/3 median response time). The final sample was 86.4% female with an average age of 19.7 years (SD = 2.71). Median completion time was 12 min.

Materials and procedure

Participants were asked to complete a privacy concern scale and a hypothetical personal information disclosure index (H-PIDI) at two time points within the same survey. The H-PIDI used all 70 items that the PIDI was drawn from and in a slightly different order (see Appendix for full list). The order of scales was the same for each

Table 2: Means and zero-order Spearman's rho correlations for measured variables

Scale (min–max)	*M*	SD	1	2	3	4
1. CFIP T1 (15–105)	85.4	13.1	–			
2. H-PIDI T1 (1–70)	25.3	16.5	−0.09	–		
3. CFIP T2 (15–105)	86.2	13.9	0.90***	−0.05	–	
4. H-PIDI T2 (1–70)	27.8	18.8	−0.04	0.84***	0.00	–
5. SDS17 (0–16)	8.1	3.3	0.21*	−0.01	0.24**	0.05
6. NFC (18–90)	57.6	8.0	0.26**	0.01	0.36***	0.05
7. Trust (3–21)	14.6	4.3	0.01	−0.07	0.01	−0.08
8. Agreeableness (8–72)	56.2	9.1	0.19*	0.01	0.21*	0.07

Note: * $P < 0.05$, ** $P < 0.01$ and *** $P < 0.001$.

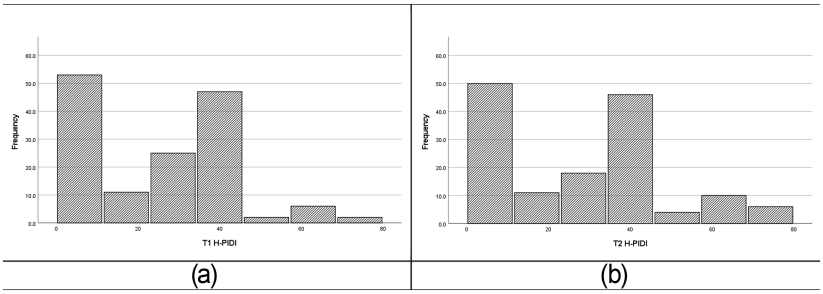

Figure 2: Frequency of H-PIDI responses at T1 (a) and T2 (b).

participant but within scale items were presented in random order (except the privacy behaviour indicator). Initially, participants were asked to complete the 15-item CFIP ($\alpha = 0.927$). Then participants were asked to indicate their hypothetical willingness to sell personal data H-PIDI as follows 'Please indicate the first item in the list below that you WOULD NOT consider selling for modest compensation'. and were offered a lottery ticket for a small (£5) lottery for each item they were willing to sell. The list included the 67 items from Study 1 starting at 'Your height' and progressing to bank details and personal beliefs, e.g. 'Your opinion on abortion'.

Participants then completed a 16-item measure of social desirability, the SDS-17 [51]. It uses true/false questions, e.g. 'I never hesitate to help someone in case of emergency' ($\alpha = 0.722$). This was followed by the need for cognition scale [50]. This is an 18-item scale on a 5-point Likert-type scale from 'extremely uncharacteristic of me' to 'extremely characteristic of me', e.g. 'I prefer complex to simple questions' ($\alpha = 0.776$). Participants then completed a 3-item general trust scale which used a 7-point Likert-type scale anchored from strongly disagree to strongly agree, e.g. 'I usually trust people until they give me a reason not to trust them' ($\alpha = 0.853$; [52]). An 8-item agreeableness scale was then presented [53]. Participants ranked themselves for accuracy of trait descriptions Extremely-inaccurate to Extremely-accurate on a 9-point Likert-type scale for traits such as 'warm' and 'kind' ($\alpha = 0.850$). Finally, the participants completed the CFIP a second time ($\alpha = 0.938$) and then completed the H-PIDI again before answering demographics and debrief questions.

Results and discussion

In line with Study 1, this investigation into privacy behaviours relating to online hypothetical information again found that participants were willing to sell more private information on the second time of asking (H-PIDI: T1 = 25.3, T2 = 27.8; t (131) = 2.73, $P = 0.007$; see also Table 2). This supports our primary hypothesis. As in Study 1, there is a wide spread of responses (see Fig. 2). Thus, the effect is robust to the change in medium (online vs. in person) and the change in question format (hypothetical vs. actual), and cannot be explained by participants disclosing false information.

We note, however, that the majority of participants sold the same at each time of asking ($n = 104$). Yet, nearly twice as many people were willing to sell more data ($n = 18$, $M = 24$, SD = 13.8) than who wished to sell less ($n = 10$, $M = -10$, SD = 11.9) at the second time of asking. Therefore, it seems reasonable that future research may be particularly interested in investigating the influence of individual differences on the propensity to share personal information.

Privacy concern increased slightly from T1 to T2 but not significantly (t (131) = 1.85, $P = 0.067$). Notably then, the increased selling of information at T2, relative to T1, does not coincide with a *reduction* in privacy concern, which could have explained the increased giving. Therefore, Study 2, as with Study 1, suggests that a foot-in-the-door mechanism is at play and that this process may contribute to the privacy paradox.

In Table 2, we present mean scores for each of the scale variables and zero-order Spearman's rho correlations. Privacy concern at T1 and T2 was predicted by social desirability, need for cognition and agreeableness measures, and the T1 and T2 scores of privacy concern correlated highly. The H-PIDI at T1 was only correlated with its T2 measure. The T2 H-PIDI was additionally marginally associated with T1 privacy concern. The reported scores are indicative and uncorrected for multiple comparisons—after Bonferroni correction only the CFIP T1 -T2 correlation, H-PIDI T1-2 correlation and NFC-CFIP-T2 correlations remain significant. No variables predicted H-PIDI change with no correlation with disclosing behaviour T1–T2 change reaching significance. There was no support for the hypotheses that NFC, agreeableness, social desirability or trust increase privacy disclosure and compliance.

It is worth noting that the H-PIDI scores in this study are notably below the PIDI scores of Study 1. While the pattern of increased responding at T2 is maintained the absolute level of disclosure appears lower. There are a number of differences between the two studies,

Table 3: Linear model of predictors of CFIP scores

	CFIP time 1			*CFIP T2*		
Variable	*B (CI)*	*SE B*	*β*	*B (CI)*	*SE B*	*β*
H-PIDI T1	−0.12 (−0.26, 0.02)	0.06	−0.15	0.03 (−0.74, 0.12)	0.06	0.03
SDS17	0.98 (0.20, 1.87)	0.44	0.25*	0.17 (−0.11, 0.49)	0.15	0.04
NFC	0.40 (0.20, 0.59)	0.12	0.24***	0.13 (0.02, 0.27)	0.06	0.08*
Trust	−0.10 (−0.71, 0.52)	0.31	−0.03	−0.03 (−0.24, 0.21)	0.10	−0.01
Agreeableness	0.09 (−0.19, 0.37)	0.13	0.06	0.13 (−0.01, 0.13)	0.06	0.01
H-PIDI T2				−0.01 (−0.10, 0.11)	0.05	−0.02
CFIP T1				0.96 (0.87, 1.02)	0.04	0.90***
R^2	0.15***			0.88***		

Note: confidence intervals are 95% BCa CI's based on 1000 bootstrap samples. * $P < 0.05$, ** $P < 0.01$ and *** $P < 0.001$.

which might account for this difference, the PIDI was hypothetical, in a different order and online rather than in person. It might be that people take more risks in reality than they would expect to hypothetically—we know that people are more subject to affect for real than hypothetical choices and the possibility of immediate gratification may have enhanced disclosure [54]. It may be that the H-PIDI, which is ordered more closely with common personal data requests introduces items that participants may be reluctant to disclose earlier. Alternatively, it may be that demand characteristics increase willingness to disclose in person—although social desirability has been found constant across modalities [55].

Four bootstrapped regressions were carried out to predict H-PIDI and CFIP at T1 and T2. At T1, the four psychometric measures (SDS17, NFC, Trust and Agreeableness) were used as well as either H-PIDI at T1 or CFIP at T1. At T2, the same measures were used as well as the other T1 predictor variable and either H-PIDI or CFIP at T2. The model for H-PIDI T1 did not reach significance [$R = 0.18$, $F\ (5126) = 0.84$, $P = 0.525$]. The model for H-PIDI at T2 [$R = 0.83$, $F\ (7124) = 40.17$, $P < 0.001$] had only one significant predictor, H-PIDI at T1 ($B = 0.94$, $SE = 0.05$, $P < 0.001$). The models for CFIP are shown in Table 3. SDS17 and NFC measures predict CFIP at T1 and at T2 only CFIP at T1 and NFC are predictive.

This study illustrates that predicting specific privacy behaviour is challenging, as we found that it was not associated with general privacy concern or personality measures. A substantive contextual element of privacy behaviour is likely to be situation specific such as perceived benefit and, in this study, prior requests.

General privacy concern as measured by CFIP was greater with increased need for cognition, and social desirability. Agreeableness was also associated with higher *concern*, however, this effect was lost when it was considered together with the other variables—possibly due to a high intercorrelation with social desirability ($r\ (135) = 0.39$, $P < 0.001$). Social desirability has been considered a factor in the disconnect between concern and behaviour—that people who wish to present themselves as concerned might not also act to protect their privacy and this is found in this data. There is likely a social component to privacy and although here that does not extend to privacy behaviour, it might be possible to exploit social motives to change behaviour. These results suggest that the privacy–behaviour gap is not only about self-presentation. Perhaps NFC, which was associated with privacy concern, can be leveraged in future interventions to inform privacy behaviour.

In summary, disclosure was greater at second request, but this was not explained by privacy concern, which did not decrease at second report. Privacy disclosure and change in privacy behaviour was not associated with the personality measures or with privacy concern. Privacy concern was predicted by need for cognition and social desirability.

General Discussion

In our digital age consumers are often faced with repeated personal information requests. Incrementally, more information is often requested on subsequent website visits including further email, telephone or personal history information. Two studies, both in the laboratory and online demonstrate increased privacy disclosure responses to a second request. This change in disclosure, analogous to a FITD effect, is not predicted by privacy concern. These studies show that while a repeated request leads to greater disclosure, this change in behaviour is not explained by privacy concern and is, therefore, not congruent with participants stated desire to maintain privacy. It is possible that exposure to repeated and incrementally escalating requests in the online world could help to create this situation, which is consistent with the privacy paradox, just as the FITD effect does not require explicit attitudinal change to affect behaviour [34]. Companies may wish to avoid accidentally or purposefully exploiting the privacy paradox via repeated requests because consumer trust underlies the personal data business model. The closure of Cambridge Analytica demonstrates what can happen when personal data collection and use goes beyond consumer expectations.

This is one of a number of factors which influence personal disclosure, which also include consideration of the benefits of disclosure, number and similarity of other disclosers, network size, self-presentation and nudges [8–12]. However, it does appear to be distinct from digital fatigue and digital resignation as it operates over a shorter timescale [37, 38]. Although there are multiple routes to personal disclosure, our understanding of them provides opportunities to assist with appropriate levels of disclosure.

Future research should consider how consumers might resist the FITD technique in online settings. Awareness that data requests can escalate may be a key. Forewarning of persuasive intent generally leads to resistance, particularly when the influence attempt is seen as self-relevant and important [56]. People who resist a weak persuasive attempt initially are better at resisting stronger requests later [57], thus training or opportunities to 'practice' rejecting data requests may allow consumers to behave in a manner that better reflects their concern for their own information privacy. It is useful to consider this in the context of privacy fatigue and bolstering people's belief in self-control and resilience over time. Even in the case where requests appear in 'novel' settings, such as in our experiments, general effects of privacy fatigue and decreased self-efficacy regarding one's data may still have an effect. A further avenue of investigation is consumer-centric—strengthening or increas-

ing the salience of one's attitudes increases the motivation and ability to resist persuasion [58]. Therefore, further investigations should examine the possibility that reinforcing one's privacy concern may lead to more congruent privacy behaviours and reduce the observed paradox.

Predicting privacy-related behaviour is challenging. In most domains, attitudes and behavioural intentions are strong predictors of actual behaviour [59], but that is generally not the case here. In two studies, we saw no relationship between privacy concern and actual or hypothetical behaviour. Even self-reports of past behaviour did not match the behaviour exhibited in our studies. However, we did see associations linking privacy behaviour to openness. A more comprehensive investigation linking privacy behaviour and with personality may be fruitful. For example, a general focus on prevention of negative outcomes [60], rather than a promotion of positive outcomes may predict engaging in privacy-protecting behaviours. Additional work could examine how businesses interact with consumers. If a company is perceived as 'tricking' consumers to give up their data, it may result in reduced engagement, lower profits or worse if the business model relies on personal data.

Future work should attempt to develop other manipulations that alter privacy behaviour, with a particular goal of examining whether or not privacy concern changes along with behaviour. Such manipulations may include other compliance techniques [61], or interventions using subtle social-norms or 'nudging' approaches [62]. Other research should focus on contextual or environmental factors that should affect the willingness to divulge sensitive information [63]. It would be interesting to examine the interaction of FITD mechanism with privacy fatigue over multiple repeated requests, as happens with repeated visits to websites over time. This will help to further elucidate the mechanisms by which the privacy paradox develops. In the longer term, such research may provide insights that would enable consumers to make better decisions about what to share when they are online.

In summary, two studies show that a FITD effect on information requests leads to increased information disclosure, while not impacting respondents' privacy concerns. Thus, we illustrate a rather simple scenario where consumers may disclose more information than they think they would like to, thereby offering a clear mechanism that contributes to the privacy paradox and a security vulnerability.

Supplementary Data

Supplementary data is available at *Cybersecurity Journal* online.

Authors' Contributions

P.F. (conceptualization, data curation, formal analysis, funding acquisition, investigation, methodology, project administration, supervision, writing—original draft and writing—review and editing); S.G.E. (conceptualization, data curation, investigation, methodology, project administration, writing—original draft and writing—review and editing); A.P.B. (conceptualization, funding acquisition, investigation, methodology, supervision, writing—original draft and writing—review and editing) and C.R.S. (conceptualization, funding acquisition, investigation, methodology, supervision, writing—original draft and writing—review and editing).

Funding

This work was supported by the Research Councils UK (www.ukri.org) via the Centre for Copyright and New Business Models in the Creative Economy (CREATe), AHRC grant number AH/K000179/1, and the University of East Anglia. The funders had no role in study design, data collection and analysis, decision to publish or preparation of the manuscript.

References

1. The Economist. The world's most valuable resource is no longer oil, but data. The Economist. 2017.
2. Greenberg CI, Firestone IJ. Compensatory responses to crowding: effects of personal space intrusion and privacy reduction. *J Pers Soc Psychol* 1977;**35**:637–44.
3. Jones H, Soltren JH. Facebook: threats to privacy. *Proj MAC MIT Proj Math Comput* 2005;**14**:1–76.
4. Nguyen KD, Rosoff H, John RS. Valuing information security from a phishing attack. *J Cybersecur* 2017;**3**:159–71.
5. Norberg PA, Horne DR, Horne DA. The privacy paradox: personal information disclosure intentions versus behaviors. *J Consum Aff* 2007;**41**:100–26.
6. Acquisti A, Grossklags J. Privacy and rationality in individual decision making. *IEEE Secur Priv Mag* 2005;**3**:26–33.
7. Acquisti A, Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information. *Science* 2015;**347**:509–14.
8. Aboulnasr K, Tran GA, Park T. Personal information disclosure on social networking sites. *Psychol Market* 2022;**39**:294–308.
9. Trepte S, Scharkow M, Dienlin T. The privacy calculus contextualized: the influence of affordances. *Comput Hum Behav* 2020;**104**:106115.
10. Krasnova H, Spiekermann S, Koroleva K. *et al.* Online social networks: why we disclose. *J Inf Technol* 2010;**25**:109–25.
11. Mouakket S, Sun Y. Examining factors that influence information disclosure on social network sites from the perspective of network externalities. *Ind Manag Data Syst* 2019;**119**:774–91.
12. Ioannou A, Tussyadiah I, Miller G. *et al.* Privacy nudges for disclosure of personal information: a systematic literature review and meta-analysis. *PLoS ONE* 2021;**16**:e0256822.
13. Waldman AE. Cognitive biases, dark patterns, and the 'privacy paradox'. *Curr Opin Psychol* 2020;**31**:105–9.
14. Freedman JL, Fraser SC. Compliance without pressure: the foot-in-the-door technique. *J Pers Soc Psychol* 1966;**4**:195–202.
15. Scott CA. Modifying socially-conscious behavior: the foot-in-the-door technique. *J Consum Res* 1977;**4**:156–64.
16. Beaman AL, Cole CM, Preston M. *et al.* Fifteen years of foot-in-the door research: a meta-analysis. *Pers Soc Psychol Bull* 1983;**9**:181–96.
17. Burger JM. The foot-in-the-door compliance procedure: a multiple-process analysis and review. *Pers Soc Psychol Rev* 1999;**3**:303–25.
18. Dillard JP, Hunter JE, Burgoon M. Sequential-request persuasive strategies. *Hum Commun Res* 1984;**10**:461–88.
19. Bem DJ. Self-perception theory. *Adv Exp Soc Psychol* 1972;**6**:1–62.
20. Burger JM, Caldwell DF. The effects of monetary incentives and labeling on the foot-in-the-door effect: evidence for a self-perception process. *Basic Appl Soc Psychol* 2003;**25**:235–41.
21. Pliner P, Hart H, Kohl J. *et al.* Compliance without pressure: some further data on the foot-in-the-door technique. *J Exp Soc Psychol* 1974;**10**:17–22.
22. Cialdini RB, Trost MR, Newsom JT. Preference for consistency: the development of a valid measure and the discovery of surprising behavioral implications. *J Pers Soc Psychol* 1995;**69**:318–28.
23. Morsella E, Zarolia P, Gazzaley A. *et al.* Cognitive conflict and consciousness. In: Gawronski B, Strack F (eds), *Cognitive Consistency: A Unifying Concept in Social Psychology*. New York City: Guilford Press, 2012, 19–46.
24. Festinger L. *A Theory of Cognitive Dissonance*. Stanford: Stanford University Press, 1962.
25. Gawronski B. Back to the future of dissonance theory: cognitive consistency as a core motive. *Soc Cogn* 2012;**30**:652–68.
26. Gilbert SJ. Another look at the Milgram obedience studies: the role of the gradated series of shocks. *Pers Soc Psychol Bull* 1981;**7**:690–5.

27. Arkes HR, Boehm LE, Xu G. Determinants of judged validity. *J Exp Soc Psychol* 1991;**27**:576–605.
28. Hawkins SA, Hoch SJ, Meyers-Levy J. Low-involvement learning: repetition and coherence in familiarity and belief. *J Consum Psychol* 2001;**11**:1–11.
29. Pascual A, Guéguen N, Pujos S. *et al.* Foot-in-the-door and problematic requests: a field experiment. *Soc Influen* 2013;**8**:46–53.
30. Patch ME. The role of source legitimacy in sequential request strategies of compliance. *Pers Soc Psychol Bull* 1986;**12**:199–205.
31. Guéguen N, Jacob C. Fund-raising on the web: the effect of an electronic foot-in-the-door on donation. *Cyberpsychol Behav* 2001;**4**:705–9.
32. Petrova PK, Cialdini RB, Sills SJ. Consistency-based compliance across cultures. *J Exp Soc Psychol* 2007;**43**:104–11.
33. Dolinski D. On inferring one's beliefs from one's attempt and consequences for subsequent compliance. *J Pers Soc Psychol* 2000;**78**:260–72.
34. Gorassini DR, Olson JM. Does self-perception change explain the foot-in-the-door effect?. *J Pers Soc Psychol* 1995;**69**:91–105.
35. Brown AS, Nix LA. Turning lies into truths: referential validation of falsehoods. *J Exp Psychol Learn Memory Cognit* 1996;**22**:1088–100.
36. Cacioppo JT, Petty RE. Effects of message repetition on argument processing, recall, and persuasion. *Basic Appl Soc Psychol* 1989;**10**:3–12.
37. Choi H, Park J, Jung Y. The role of privacy fatigue in online privacy behavior. *Comput Hum Behav* 2018;**81**:42–51.
38. Draper NA, Turow J. The corporate cultivation of digital resignation. *New Media Soc* 2019;**21**:1824–39.
39. Barry B, Friedman RA. Bargainer characteristics in distributive and integrative negotiation. *J Pers Soc Psychol* 1998;**74**:345–59.
40. Taylor JF, Ferguson J, Ellen PS. From trait to state: understanding privacy concerns. *J Consum Market* 2015;**32**:99–112.
41. Osatuyi B. Personality traits and information privacy concern on social media platforms. *J Comput Inf Syst* 2015;**55**:11–9.
42. Mneimneh ZM, Tourangeau R, Pennell B-E. *et al.* Cultural variations in the effect of interview privacy and the need for social conformity on reporting sensitive information. *J Off Stat* 2015;**31**:673–97.
43. Hermstrüwer Y, Dickert S. Tearing the veil of privacy law: an experiment on chilling effects and the right to be forgotten. MPI Collective Goods Preprint. Bonn: Max Planck Institute for Research on Collective Goods, 2013.
44. Smith HJ, Milberg SJ, Burke SJ. Information privacy: measuring individuals' concerns about organizational practices. *MIS Quart* 1996;**20**:167–96.
45. Buchanan T, Paine C, Joinson AN. *et al.* Development of measures of online privacy concern and protection for use on the Internet. *J Am Soc Inf Sci Technol* 2007;**58**:157–65.
46. Gosling SD, Rentfrow PJ, Swann WB. A very brief measure of the Big-Five personality domains. *J Res Pers* 2003;**37**:504–28.
47. Reynolds WM. Development of reliable and valid short forms of the Marlowe-Crowne social desirability scale. *J Clin Psychol* 1982;**38**:119–25.
48. Jentzsch N, Preibusch S, Harasser A. Study on monetising privacy: an economic model for pricing personal information. Attiki: ENISA, 2012.
49. Joinson AN, Reips U-D, Buchanan T. *et al.* Privacy, trust, and self-disclosure online. *Hum-Comput Interact* 2010;**25**:1–24.
50. Cacioppo JT, Petty RE, Feng Kao C. The efficient assessment of need for cognition. *J Pers Assess* 1984;**48**:306–7.
51. Stöber J. The social desirability scale-17 (SDS-17). *Eur J Psychol Assess* 2001;**17**:222–32.
52. McKnight DH, Kacmar CJ, Choudhury V. Dispositional trust and distrust distinctions in predicting high-and low-risk internet expert advice site perceptions. *e-Service J* 2004;**3**:35–55.
53. Saucier G. Mini-markers: a brief version of Goldberg's unipolar Big-Five markers. *J Pers Assess* 1994;**63**:506–16.
54. Isen AM, Patrick R. The effect of positive feelings on risk taking: when the chips are down. *Organ Behav Hum Perform* 1983;**31**:194–202.
55. Dodou D, de Winter JCF. Social desirability is the same in offline, online, and paper surveys: a meta-analysis. *Comput Hum Behav* 2014;**36**:487–95.
56. Wood W, Quinn JM. Forewarned and forearmed? Two meta-analysis syntheses of forewarnings of influence appeals. *Psychol Bull* 2003;**129**:119–38.
57. McGuire WJ, Papageorgis D. The relative efficacy of various types of prior belief-defense in producing immunity against persuasion. *J Abnormal Soc Psychol* 1961;**62**:327–37.
58. Petty RE, Cacioppo JT, Goldman R. Personal involvement as a determinant of argument-based persuasion. *J Pers Soc Psychol* 1981;**41**:847–55.
59. Ajzen I, Fishbein M. *Understanding Attitudes and Predicting Social Behaviour*. Englewood Cliffs: Prentice-Hall, 1980.
60. Higgins ET. Promotion and prevention: regulatory focus as a motivational principle. In: Zanna MP (ed.), *Advances in Experimental Social Psychology*. **Vol. 30**. New York: Elsevier, 1998, 1–46.
61. Cialdini RB, Goldstein NJ. Social influence: compliance and conformity. *Annu Rev Psychol* 2004;**55**:591–621.
62. Thaler R, Sunstein C. *Nudge: The Gentle Power of Choice Architecture*. New Haven: Yale University Press, 2008.
63. John LK, Acquisti A, Loewenstein G. Strangers on a plane: context-dependent willingness to divulge sensitive information. *J Consum Res* 2011;**37**:858–73.

Appendix

Tell Me More, Tell Me More: Repeated Personal Data Requests Increase Disclosure.

Questions from 'Perceptions of intrusion', adjusted for experiment—Study 1 PIDI.

Please answer the below questions.

Please note: your responses to the below will be used in the second part of the experiment, where you will make decisions on whether to 'sell' some items for modest compensation. Each sold item will be publicised on a purpose-made website for up to 4 weeks. Important: for half the participants (this could be you) the sale decisions, and therefore, the money you receive and the amount of your information that it put online will be based on the judgements of another participant. Therefore, only answer questions that you would genuinely consider agreeing to receive compensation for the publicization of.

1. How do you classify your gender?
2. How would you describe your ethnicity?
3. What is your height?
4. Which company is your internet provider?
5. What mobile phone do you currently own?
6. Please list the social media accounts that you have signed up to.
7. Please describe the content of your last five Facebook posts (or as many as you can remember).
8. Please list any membership of extracurricular groups/teams/societies.
9. What is your date of birth?
10. Which company is your mobile phone network provider?
11. Where were you born?
12. How do you rate your current course of study/job?
13. Would you rather move to live somewhere else than your current place of residence?
14. Provide the names of any siblings (or other non-parental family).
15. How often do you visit family (e.g. on average per month)?
16. What is your least favourite nickname?
17. What are your parents names?
18. What is your relationship status?
19. How many hours per week do you spend studying (either academically or out of personal interest)?
20. What do you consider to be your most recent success?
21. What do you consider to be your biggest success?
22. In an average week, how much alcohol do you consume?
23. How many times per month do you call family?
24. Which bank do you use?
25. What is your sexual orientation?
26. What is your opinion regarding homosexuality?
27. What is your perspective on religion?

28. Over the past month, how many important conversations have you had with friends?
29. Please provide your username for as many social media accounts as you can.
30. What is your opinion on immigration?
31. Which political party did you last vote for (or if you have not voted before—who are you most likely to vote for)?
32. Who do you text most often?
33. What is your opinion on abortion?
34. What is your opinion on euthanasia?
35. What is your email address?
36. What was your address prior to your current address?
37. What is your current/most recent average academic grade?
38. What is your biggest fear?
39. What do you consider to be your most recent failure?
40. What is your current weight?
41. Have you ever cheated academically?
42. Specify someone that you have looked up on social media in the last month.
43. What is your most embarrassing habit?
44. What do you consider to be your biggest failure?
45. What is your phone number (mobile)?
46. How often do/did arguments occur between yourself and your current/most recent partner?
47. What is your phone number (landline)?
48. Over the last month, how often have you used social media to 'stalk' others?
49. What is your honest opinion of your current/most recent housemates?
50. Detail any history of illegal drug use.
51. What is your current residential address?
52. Who do you currently find attractive/fantasize about?
53. What was the reason for your most recent relationship ending?
54. Have you ever been romantically unfaithful?
55. Please list any currently or previously prescribed medications.
56. List the websites you have visited in the last month.
57. What was the topic of your last conversation via instant messaging?
58. What is the biggest lie you have ever told?
59. State any history of psychological problems.
60. List the google searchers you have made over the last month.
61. What is/was your parents' income?
62. What is your most painful memory?
63. What is your current bank balance?
64. How often do you have (or did you have) intercourse with your current (or previous) partner?
65. Describe a sexual fantasy.
66. Please provide your Facebook log-in details (username and password).
67. What is your bank account number?

Study 2 Full 70-item H-PIDI

1. How tall are you?
2. How much do you weigh?
3. What is your date of birth?
4. Where were you born?
5. What is your gender?
6. What is your ethnicity?
7. What is your email address?
8. What is your phone number?
9. What is your current residential address?
10. What was your last address (prior to your current address)?
11. How often do you visit family (on average per month)?
12. How frequently do you (phone) call family (on average per month)?
13. What is your current academic grade (average percent)?
14. Have you ever cheated (academically)?
15. Are you in paid employment while studying?
16. How many hours per week do you spend studying/working?
17. Where do you work (name of organization)?
18. What extracurricular groups/teams/societies are you currently a member of?
19. How much alcohol do you consume per week (on average)?
20. What is your relationship status?
21. What is your sexual orientation?
22. What were the reasons for your previous relationship breakups?
23. How often do/did you argue(d) with your current or previous partner?
24. What is/was your frequency of sexual intercourse with current/previous partner?
25. Have you ever been unfaithful (romantically)?
26. What were your last five Facebook posts about?
27. What were your last five conversations via instant messaging about?
28. How many important conversations you have had with university friends in the last month?
29. How many important conversations you have had with friends from before university in the last month?
30. What is your honest opinion of your current housemates?
31. Would you rather move to live elsewhere?
32. What is your most embarrassing habit?
33. What social media accounts do you have (e.g. Twitter, Facebook)?
34. What are your username for your various social media accounts (e.g. Twitter, Facebook)?
35. How often have you have used social media to 'stalk' others in the last month?
36. Who have you looked-up on social media in the last month?
37. What are your social media login details (username and password) for the account you use most often (e.g. Facebook)?
38. Which bank do you use?
39. What is your current bank balance?
40. What is your back account number?
41. What is your mobile phone number?
42. Which company is your mobile phone network provider?
43. Which company is your internet network provider?
44. Who do you text the most?
45. What medication have you most recently been prescribed?
46. Which illegal drugs have you used?
47. Do you have a history of psychological problems?
48. What is your biggest fear?
49. What is your least favourite nickname?
50. What is he biggest lie you have ever told?
51. How do you rate your current course of study?
52. Which political party did you last/will you next vote for?
53. What are the last five things you searched for (e.g. google?)
54. What five websites have you visited most in the last month?
55. What mobile phone do you currently have?
56. What do you consider to be your most recent success?
57. What do you consider to be your most recent failure?
58. What do you consider to be your biggest success?
59. What do you consider to be your biggest failure?
60. What is your opinions of homosexuality?
61. What is your most painful memory?
62. Who do you currently find attractive/fantasise about?
63. What sexual fantasies do you have?
64. What is your perspective on religion?
65. What are your opinions on immigration?
66. What are your opinions on abortion?
67. What are your opinions on euthanasia?
68. What are the names of your parents?
69. What are the names of your siblings (or other non-parent family members)?
70. What is your parents' income (approximately)?