Journal of Behavioral Economics for Policy, Vol. 5, Issue 1, 45-52, 2021

Nudging online privacy behaviour with anthropomorphic cues

Nuria Rodríguez-Priego[1,2], René van Bavel[1]*, Shara Monteleone[1]

Abstract
Personal data is often considered the currency of the digital world, allowing companies to better control, study and target consumers. However, users may not always be aware they are disclosing personal data online, posing a privacy policy problem. We tested whether the display of anthropomorphic cues could curb users' unwitting disclosure of personal information. We conducted an online experiment with a between-subject design in Germany, Italy, Poland, and the UK (n=1,217). Neither a 'static' nor a 'dynamic' anthropomorphic character made participants disclose less personal information – in fact, the static character made them disclose more (p=0.03). Findings are interpreted by considering the effect of anthropomorphic characters on trust, which may in turn increase disclosure. Level of education and country also influenced disclosure.

JEL Classification: D18; D90; D91

Keywords
Privacy behaviour — behavioural economics — personal data — nudges — avatars — trust

[1] *Joint Research Centre, European Commission, Seville, Spain*
[2] *Department of Economic Analysis, Autonomous University of Madrid, Madrid, Spain*
*__Corresponding author__: rene.van-bavel@ec.europa.eu

Introduction

Electronic commerce implies collecting personal information from consumers. Sellers need this information to develop customer profiles and offer personalized products and services. From policy point of view, privacy concerns are prominent, as online service providers increasingly gain access to potentially sensitive consumer information, which they may share or misuse. Here, we are interested in policy options, relying on behavioural insights, which may lead users to exercise caution when disclosing their data.

Self-disclosure traditionally refers to the voluntary and intentional action of revealing personal information, feelings, attitudes, or experiences (Qian & Scott, 2007; Krasnova et al., 2010). However, individuals sometimes disclose personal information without even realizing they are doing so (Wu et al., 2012). This element of unconscious self-disclosure undermines the principle of requiring informed consent before personal data is processed, which is one way various privacy regulatory regimes (such as the EU's) seek to protect users.[1] It also suggests that policy options following the behavioural insights principle of 'changing behaviour without changing minds' could be appropriate (Dolan et al., 2012).

A growing stream of behavioural research (Acquisti & Grossklags, 2007) has focused on the role of cognitive biases and heuristics in privacy decision-making, highlighting how otherwise privacy conscious and sensitive individuals may end up engaging in potentially risky disclosure of personal data (i.e. the 'privacy paradox'). Privacy behaviour is highly context-dependent and can be easily influenced, or nudged, by changes in the choice architecture (Acquisti et al., 2015; Bansal et al., 2016; Thaler & Sunstein, 2008). For example, nudges can influence disclosure behaviour by making individuals more comfortable with an online environment, or by setting privacy-protecting features as a default (Dogruel et al., 2017). These nudges can be alternative and complementary policy measures for privacy and personal data protection, relying on 'soft paternalism' instead of strict regulation (Acquisti, 2009, 2010; Acquisti et al., 2015; Acquisti et al., 2017; Calo, 2012; Groom & Calo, 2011; John et al., 2010).

Anthropomorphic cues as nudges

We conducted an online experiment measuring the effect of an anthropomorphic character on unwitting disclosure of personal data in a privacy-sensitive scenario. Anthropomorphism – or the use of an object that imitates human qualities and features within an inanimate object (Schmitz, 2011) – is often applied to digital interfaces. It is intended to increase engagement, interaction and social presence by users with a software, application, or online platform, and can help users become more familiar with the functions and services being offered (Mohd et al., 2016; Araujo, 2018). Examples of such human-like characters are Microsoft Windows' animated paperclip or IKEA's virtual assistant Anna.

[1] See ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en for an overview of the main elements of the EU's General Data Protection Regulation.

Set	Item	Sensitive
1	Find a recipe for chocolate cake and list all the ingredients	No
	Provide the name of the winner at the Eurovision song contest in 1978	No
	Provide the name of a famous public figure or celebrity born the same year as you	Yes
2	In what year was the bank you use founded?	Yes
	Which years marked the beginning and the end of the Crimean War?	No
	Which Shakespeare play was first performed in 1604?	No
3	What are the names of three of the moons of Neptune?	No
	What is the full name of the 81st element in the periodic table?	No
	What is the address of your favourite restaurant located in the town where you were born?	Yes

Table 1. Sets of three questions (including a sensitive one)

When people interact with a technology presenting characteristics associated with human behaviour, they respond by exhibiting social behaviours and making social attributions (Nass et al., 1995; Moon & Nass, 1996). Anthropomorphic cues in computer interfaces remind users of human agency and trigger a mindless response to computers as if they were social actors (Reeves & Nass, 1996; Bailenson et al., 2001). From a design perspective, these cues do not have to be highly sophisticated to elicit social presence, i.e. the feeling of being with another person (Biocca et al., 2003; Bente et al., 2004; Sundar et al., 2008; Kim & Sundar, 2012).

Evidence suggests people reveal less personal information when dealing with humans than with a machine. For example, automated virtual humans increase willingness to disclose health information compared to virtual agents controlled by a human operator (Lucas et al., 2014). Participants are more honest with the 'impartial machine' and provide embarrassing information, as they probably do not fear a negative evaluation of their behaviour. Along these lines, including images of eyes on websites is associated with an increase in pro-social behaviour and donations (Powell et al., 2012), due to a feeling of being monitored. Overall, anthropomorphic cues increase users' public self-awareness (Joinson, 2001; Sah & Peng, 2015), and should therefore lead to more prudent disclosure (Groom & Calo, 2011; Moon, 2000). Hence our first hypothesis:

> **H1:** Participants who are exposed to a human-like agent will disclose less personal information than participants who are not exposed to a human-like agent.

We were also interested in testing the additional effect of increasing the realism of the anthropomorphic character. The literature suggests that characters with greater behavioural realism produce higher levels of social presence than characters with a lower level of realism (Bailenson et al., 2002). More specifically, we tested the effect of a human-like character whose eyes followed the cursor as it moved around, heightening the feeling of being observed. This dynamic element to the human-like character should exacerbate its effect on personal data disclosure, because of a presumably strengthened surveillance effect. Our second hypothesis was therefore:

> **H2:** Participants who are exposed to a dynamic human-like agent will disclose less personal data than participants who are exposed to a static human-like agent.

Material and methods

Procedure

We conducted an online experiment with a between-subject randomised design. We collected the data through a series of subject panels managed by Harris International, a social research company. We invited participants to an online study and asked them to interact with a mock online search engine. During the interaction with the search engine they could make choices that would disclose personal data (unwittingly to them).

We asked participants to evaluate the mock search engine by searching for the answers to seven questions. The first four questions were about general knowledge and answering them was compulsory in order to continue with the experiment. Next came three sets of three questions each, and participants had to choose one per set. In each set, we designed one of the three questions in such a way that participants would reveal personal information if they answered it (a 'sensitive' question; Table 1). Choosing to answer such a question was a measure of participants' unwitting disclosure of personal information. We could not be certain if participants were disclosing true or false personal information, a limitation inherent to such experiments (Keith et al., 2013). However, we were interested in whether the treatments affected personal information disclosure, no matter if this information was truthful or not, as what users reveal is the starting point for online businesses to personalize their services and profile their customers.

The mock search engine was a website interface connected to an existing search engine; no new search technology was

Treatment	Description	Passive disclosure				
		Mean	SD	Min	Max	N
Control	Dummy variable equal to 1 if the participant visualizes the control treatment.	0.50	0.50	0	1	419
Dynamic	Dummy variable equal to 1 if the participant visualizes the dynamic treatment	0.57	0.50	0	1	383
Static	Dummy variable equal to 1 if the participant visualizes the static treatment	0.59	0.49	0	1	415

Table 2. Description of treatments

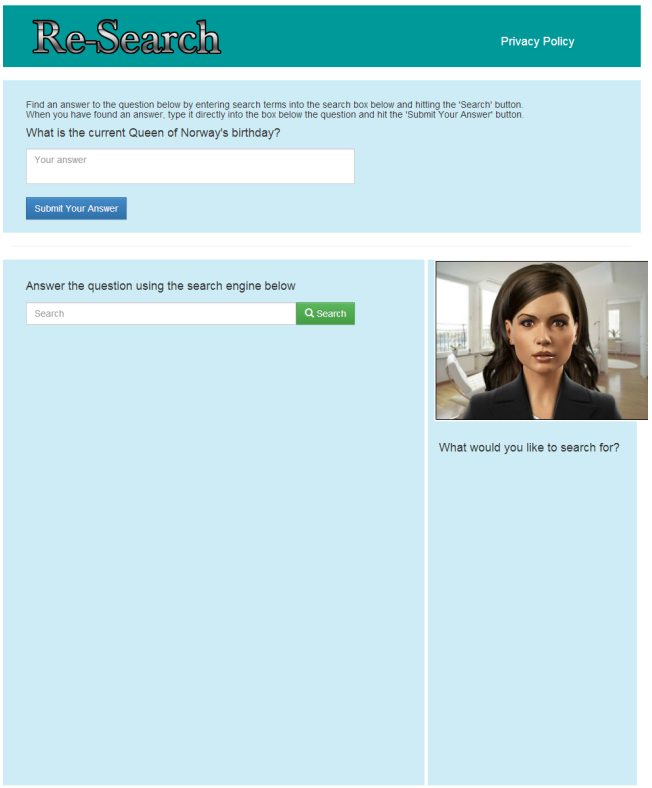

Figure 1. Screenshot of static anthropomorphic condition

actually created. Participants were debriefed about this aspect of the study at the end of the experiment. The mock search engine was named 'Re-Search Engine' and had a logo, a box for inserting the search query, and an area for displaying search results. The search engine interface was translated into the different languages of the four countries selected. It was also adapted and modified according to the needs of the two experimental treatments.

During the search process, the mock search engine directed participants to existing external webpages. They returned to the mock search engine website once they had found the answers to the search queries in order to continue with the experiment. The questions appeared above the search box. Below the search box, participants could type their answers in another box.

Main outcome measure

We measured participants' passive disclosure of personal information by recording whether they chose to answer a sensitive question, thus revealing personal information, after answering the four compulsory general knowledge questions. They scored zero for *passive disclosure* if they managed to avoid the sensitive questions and one if they chose a sensitive question. The variable was binary and not continuous (i.e. from one to three, depending on the number of sensitive questions) because the key question was whether they were alert or careful enough to avoid selecting a question that made them reveal personal information. A priori, the personal information that the different sensitive questions obtained was assumed to be equally concerning. For the purposes of the study, the main point was that, compared to the non-sensitive questions, they made participants reveal personal information. Answering one such question indicated the participant had failed to protect their privacy.

Experimental treatments

We randomly assigned participants to three different experimental groups (see Table 2).

- *Control condition:* The search engine's website was designed to have an ordinary corporate appearance similar to the one used by other search tools.
- *Static anthropomorphic condition:* Same as the control condition, but with the image of a woman with the look of a customer service agent and a link to the website's privacy policy. She was shown from the shoulders up in the right-hand column, close to the search bar. The words 'what would you like to search for?' appeared beneath it (Figure 1).
- *Dynamic anthropomorphic condition:* the image of the customer service agent was the same as the static anthropomorphic condition, except that it could move its head and followed the cursor's movement with its eyes.

Results

Participants

We recruited a sample of around 300 participants per country in Germany, Italy, Poland and the UK (n=1,217; Table 3). We

chose these countries to represent, to the degree that it was possible given limited resources, the geographical and cultural variety of Europe. The online experiment lasted an average of 23 minutes.

	Country			
	Germany	Italy	Poland	UK
Gender				
Female	54	47	49	45
Male	46	53	51	55
Age				
18-25	14	22	20	8
26-33	12	17	18	13
34-41	13	19	20	15
42-49	17	19	16	16
50-57	21	9	14	17
58-65	16	11	10	17
66 and above	7	3	2	14
Education level				
Below high school	5	5	1	2
Some high school	38	3	7	9
High school graduate	19	39	37	24
Some college	10	23	11	18
College graduate	24	23	37	29
Advanced degree	4	7	7	18

Table 3. Frequencies for socio-demographic characteristics (relative values)

Analysis

We conducted a logit regression to test our hypotheses with the statistical software STATA 14.0. Our outcome variable was *passive disclosure*. The dynamic and static conditions were included as dummy variables. To test H1, we used the control group as the baseline treatment. We tested for differences between the control group and the dynamic condition, and between the control group and the static condition. To test H2, we ran the same regressions, but with the static group as the baseline condition. In the regressions, we initially included country, sex, education and age as control variables. Education and age were ordinal variables. Italy was the baseline for country, meaning that any significant effect by country was in relation to Italy. Out of these, only country and education were significant. We also considered the interactions between all the control variables and the treatments. We found no interaction effect. Therefore, we eliminated the non-significant variables and conducted a final logit regression.

Results showed that, all else being equal, participants exposed to the static anthropomorphic character were *more* likely to answer at least one sensitive question, compared to the control condition (b = .30, p = .033, OR = 1.36 (95%CI: -.03, .59)). In other words, a participant visualizing the static anthropomorphic character was 1.4 times more likely to disclose personal information than a participant in the control condition. However, there were no significant differences between the dynamic anthropomorphic character and the control condition (Table 4). H1 is not supported. We tested the effect size of the difference between the static anthropomorphic character and the control condition by computing Cohen's *d* and found a small effect size (Cohen's $d = (.76 - .71)/.79 = .06$). As a robustness check, we tried testing *passive disclosure* as a count variable (from 1 to 3) in a poisson regression. We found no significant effects for the static or dynamic character. We concluded that the treatment effect of the static anthropomorphic character was small and required confirmation in further studies.

Education had a significant negative effect. Participants with a lower level of education failed to protect their personal information compared to participants with a higher level of education (b = -.14, p = .002, OR = .87 (95%CI: -.24, -.05)). For each increase in education level, participants were at lesser odds of passively disclosing information. With regard to country, participants from Italy were more likely to disclose information passively, compared to participants from Germany, Poland or the UK. However, when we rotated the baseline country, we found no significant differences between the other three countries.

Finally, we tested for multicollinearity using the variance inflation factor (VIF) and tolerance (1/VIF). A value greater than 10 for the VIF and lower than 0.1 for the tolerance means that the variables may merit further investigation. In this case, we found no multicollinearity between the variables of the model (Table 5).

In order to test H2, we rotated the baseline treatment to the static anthropomorphic condition and replicated the logit regression (Table 6). The rest of the variables were the same. Results showed no difference between the static and the dynamic anthropomorphic characters. H2 is not supported. However, we tested for differences in the *feeling of being observed*, a variable measured in a post-experiment questionnaire through a 7-point Likert scale (ranging from 1=Not at all to 7=Very much). We found statistically significant differences between the dynamic and static conditions (p=.045). Participants who visualized the dynamic anthropomorphic cue felt slightly more observed (M = 3.53, SD = 1.89) than participants who visualized the static one (M=3.26, SD=1.90).

Conclusions

We set out to test the effect of anthropomorphic cues on unwitting disclosure of personal information. Results showed that a static character led to greater disclosure, but not so a dynamic character (which moved its head and followed the cursor with its eyes).

These results were unexpected. Our first hypothesis (H1) was that anthropomorphic characters should lead to less in-

Source	Obs. Coefficient	Coeff. Std. Err.	z	P > | z |	Normal-based [95% Conf. Interval]	
Treatment						
Dynamic	0.251	0.147	1.71	0.087	-0.036	0.539
Static	0.306	0.143	2.14	**0.033**	0.025	0.587
Country						
Germany	-0.482	0.175	-2.75	**0.006**	-0.827	-0.138
Poland	-0.538	0.172	-3.12	**0.002**	-0.876	-0.200
UK	-0.557	0.171	-3.25	**0.001**	-0.894	-0.221
Education	-0.143	0.047	-3.06	**0.002**	-0.236	-0.052
Cons	0.970	0.233	4.15	0.000	0.511	1.428

LR $chi^2(6)$ = 30.70 Prob>chi^2 = 0.0000 Log likelihood = -793.26352 Pseudo R^2 = 0.0190

Table 4. Logit regression for *passive disclosure*

Variable	VIF	1/VIF
Dynamic	1.31	0.761
Static	1.31	0.761
Country	1.08	0.929
Education	1.08	0.930
Mean VIF	1.20	

Table 5. Variance inflation factor and tolerance

formation disclosure because they elicit a feeling of being observed. The dynamic characters, whose eyes followed the cursor, should have exacerbated this feeling (H2). The fact that the result of the static character was the opposite, and the absence of a significant result for the dynamic character, compared to the control or to the static character, invites a different interpretation.

Trust might be a relevant factor. Research has shown that anthropomorphic cues help build online trust (Gefen & Straub, 2004; Hassanein & Head, 2007; Hess et al., 2009; Qiu & Benbasat, 2009; Sung & Mayer, 2012; Bente et al., 2014; Etemad-Sajadi, 2016). Increased trust, in turn, leads to greater information disclosure (McKnight et al., 2002; Malhotra et al., 2004; Liu et al., 2016; Liu et al., 2019). A study by Spiekermann et al. (2001), for example, showed how participants got drawn into communications with an anthropomorphic 3-D bot and ended up revealing large amounts of highly personal information. In fact, some claim trust is the most important influence on disclosure, since it reduces the perceived risks of revealing personal information. This is something information-collecting entities know about and use to their advantage (Veltri & Ivchenko, 2017). Therefore, the static anthropomorphic character might have had a positive effect on information disclosure because of its effect on trust.

The fact that that the dynamic character did not have an effect on information disclosure suggests that two effects might be at play: the increased trust effect (as with the static character) and the surveillance effect (due to its more prominent gaze). These opposite effects could have offset each other. Given the degree of significance of the effects, prudence dictates that further iterations of this experiment are required to replicate and validate them. Further experiments should also seek to isolate and include trust as a possible contributing factor, and so attempt to disentangle both posited counteracting effects.

Our experimental design has some limitations that future research should take into account. The effect of anthropomorphic cues might vary depending on the features of the character. Hence, a manipulation check conducted before running the experiment would provide further information on how participants perceive the stimulus, especially with regard to the level of anthropomorphism and feeling of surveillance. Moreover, to increase external validity, the study could have tested anthropomorphic cues in a different context, such as a service provider's website, where it is more usual to find this type of stimuli.

A first implication of our findings is that, for policy-making with respect to privacy, nudges could change behaviour in ways that are consistent with users' preferences or that objectively increase their well-being (Acquisti et al, 2017). Here, changes to the features of website design would constitute 'soft' policy options influencing automatic and habitual behaviour, and could complement hard regulation and initiatives relying on more reflective behaviour, such as privacy notices (Kahneman, 2011).

A second implication is that online service providers can take advantage of nudging for greater personal information disclosure. They can use it to better target the consumer, which might be good for business (Acquisti et al., 2015; Veltri & Ivchenko, 2017). From a policy perspective, however, this

Source	Obs. Coefficient	Coeff. Std. Err.	z	P > | z |	Normal-based [95% Conf. Interval]	
Treatment						
Dynamic	-0.055	0.147	-0.37	0.709	-0.344	-0.234
Control	-0.306	0.143	-2.14	**0.033**	-0.587	-0.025
Country						
Germany	-0.482	0.175	-2.75	**0.006**	-0.827	-0.138
Poland	-0.538	0.172	-3.12	**0.002**	-0.876	-0.200
UK	-0.557	0.171	-3.25	**0.001**	-0.894	-0.221
Education	-0.143	0.047	-3.06	**0.002**	-0.236	-0.052
Cons	0.970	0.233	4.15	0.000	0.511	1.428

LR $chi^2(6)$ = 30.70 Prob>chi^2 = 0.0000 Log likelihood = -793.26352 Pseudo R^2 = 0.0190

Table 6. Logit regression for *passive disclosure* (Static condition as baseline)

is something to look out for and possibly monitor. These nudges need to conform to current regulations concerning unfair commercial practices or privacy protection. This is the other way policy-making needs to consider nudges, namely seeking to limit the damage caused by nudging that does not have the user's best interests at heart. The response to private or negative nudges (Carolan & Spina, 2015) need not be a nudge, but rather good regulation (Troussard & van Bavel, 2018).

A secondary finding was that information disclosure also varied according to country and level of education. The fact that participants in Italy were more likely to disclose personal information is intriguing and consistent with the observation of strong cultural effects on privacy behaviour (Acquisti et al., 2015). In addition, less educated individuals unwittingly disclosed a greater amount of personal information. This result confirms what could be reasonably expected: less-educated participants are perhaps less technologically savvy, less aware of online data gathering practices, and therefore less cautious when it comes to disclosing personal information. The result is in line with recent findings which show that greater experience with the Internet leads to greater online privacy literacy, and consequently to more cautious privacy behaviour (Bartsch & Dienlin, 2016). They also corroborate the finding that young adults aspire to increased privacy, contrary to the belief that they do not care about it (Hoofnagle et al., 2010). Finally, they support the emphasis given, at policy level, to addressing the online vulnerability of certain sectors of the population. Sometimes vulnerable people are simply not aware they are disclosing personal information – no wonder, therefore, that they do not take any steps to protect their privacy.

Acknowledgments

We are grateful to Alessandro Acquisti, Norberto Andrade, Ryan Calo, Néstor Duch-Brown, Gabriele Esposito, Ioannis Maghiros and Aaron Martin for their advice and support. The study was conducted and funded by the Joint Research Centre. The views expressed in this article are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

References

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *Security & Privacy, 7*(6). 82-85.

Acquisti, A. (2010). "From the economics to the behavioral economics of privacy: A note." *Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, ICEB 2010 Hong Kong, January 4-5, 2010*, 23-26.

Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy. *Digital Privacy: Theory, Technologies and Practices, 18*, 363-377.

Acquisti, A., Adjerid, I., Balebako, R.H., Brandimarte, L., Cranor, L.F., Komanduri, S., et al. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR), 50*(3), 44.

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

Araujo, T. (2018). Living up to the chatbot hype: The influence of anthropomorphic design cues and communicative agency framing on conversational agent and company perceptions. *Computers in Human Behavior, 85*, 183-189.

Bailenson, J. N., Beall, A. C., & Blascovich, J. (2002). Mutual gaze and task performance in shared virtual environments. *Journal of Visualization and Computer Animation, 13*, 1-8.

Bailenson, J. N., Blascovich, J., Beall, A. C., & Loomis, J. M. (2001). Equilibrium theory revisited: Mutual gaze and personal space in virtual environments. *Presence: Teleoperators & Virtual Environments, 10*(6), 583–598.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21.

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behaviour, 56*, 147-154.

Bente, G., Dratsch, T., Rehbach, S., Reyl, M., & Lushaj, B. (2014). "Do you trust my avatar? Effects of photo-realistic seller avatars and reputation scores on trust in online transactions." In *HCI in Business* (pp. 461-470). Springer International Publishing.

Bente, G., Rüggenberg, S., Tietz, B., & Wortberg, S. (2004). "Measuring behavioral correlates of social presence in virtual encounters." *54th Annual Conference of the International Communication Association*.

Biocca, F., Harms, C., & Burgoon, J. K. (2003). Toward a more robust theory and measure of social presence: Review and suggested criteria. Presence: *Journal of Teleoperators and Virtual Environments, 12*(5), 456–480.

Calo, R. (2012). Against Notice Skepticism in privacy and elsewhere. *Notre Dame Law Review, 87*, 1027-1072.

Carolan, E., & Spina, A. (2015). *Behavioural sciences and EU data protection law: Challenges and opportunities.* Nudge and the Law. Oxford: Hart Publishing.

Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. (2012). Influencing behaviour: The mindspace way. *Journal of Economic Psychology, 33*(1), 264-277.

Dogruel, L., Joeckel, S., & Vitak, J. (2017). The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. *Computers in Human Behavior, 77*, 230-239.

Etemad-Sajadi, R. (2016). The impact of online real-time interactivity on patronage intention: the use of avatars. *Computers in Human Behavior, 61*, 227-232.

Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-commerce and the importance of social presence: experiments in e-products and e-services. *Omega, 32*(6), 407-424.

Groom, V., & Calo, M. R. (2011). Reversing the privacy paradox: An experimental study. *TPRC Conference proceedings*, available at SSRN: ssrn.com/abstract=1993125 .

Hassanein, K., & Head, M. (2007). Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *International Journal of Human-Computer Studies, 65*(8), 689-708.

Hess, T. J., Fuller, M., & Campbell, D. E. (2009). Designing interfaces with social presence: using vividness and extraversion to create social recommendation agents. *Journal of the Association for Information Systems, 10*(12), 889-919.

Hoofnagle, C.J., King, J., Li, S. and Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *SSRN Electronic Journal*, available at: ssrn.com/abstract=1589864.

John, L. K., Acquisti, A., & Loewenstein, G. (2010). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research, 37*(5), 858-873.

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology, 31*(2), 177-192.

Kahneman, D. (2011). *Thinking, fast and slow.* Penguin.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies, 71*(12), 1163-1173.

Kim, Y., & Sundar, S. S. (2012). Anthropomorphism of computers: Is it mindful or mindless? *Computers in Human Behavior, 28*(1), 241-250.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109-125.

Liu, Z., Min, Q., Zhai, Q., & Smyth, R. (2016). Self-disclosure in Chinese micro-blogging: A social exchange theory perspective. *Information & Management, 53*(1), 53-63.

Liu, Z., Wang, X., & Liu, J. (2019). How digital natives make their self-disclosure decisions: a cross-cultural comparison. *Information Technology & People, 32*(3), 538-558.

Lucas, G. M., Gratch, J., King, A., & Morency, L. P. (2014). It's only a computer: Virtual humans increase willingness to disclose. *Computers in Human Behavior, 37*, 94-100.

Malhotra, N.K., Kim, S.S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355.

McKnight, D.H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for E-Commerce: An Integrative Typology. *Information Systems Research, 13*(3), 334-359.

Mohd Tuah, N., Wills, G., & Ranchhod, A. (2016). The characteristics and application of anthropomorphic interface: A design spectrum. ACHI 2016: *The Ninth International Conference on Advances in Computer-Human Interactions.*

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research, 26*(4), 323-339.

Moon, Y., & Nass, C. (1996). How "real" are computer personalities? Psychological responses to personality types in human-computer interaction. *Communication research, 23*(6), 651-674.

Nass, C., Moon, Y., Fogg, B. J., Reeves, B., & Dryer, D. C. (1995). Can computer personalities be human personalities? *International Journal of Human-Computer Studies, 43*(2), 223-239.

Powell, K. L., Roberts, G. & Nettle, D. (2012). Eye images increase charitable donations: Evidence from an opportunistic field experiment in a supermarket. *Ethology, 118*(11), 1096-1101.

Qian, H., & Scott, C. R. (2007). Anonymity and self-disclosure on weblogs. *Journal of Computer-Mediated Communication, 12*(4), 1428-1451.

Qiu, L., & Benbasat, I. (2009). Evaluating anthropomorphic product recommendation agents: A social relationship perspective to designing information systems. *Journal of Management Information Systems, 25*(4), 145-182.

Reeves, B., & Nass, C. I. (1996). *The media equation: How people treat computers, television, and new media like real people and places*. Cambridge, UK: Cambridge University Press.

Sah, Y. J., & Peng, W. (2015). Effects of visual and linguistic anthropomorphic cues on social perception, self-awareness, and information disclosure in a health website. *Computers in Human Behavior, 45*, 392-401.

Schmitz, M. (2011). "Concepts for life-like interactive objects." In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction*, (pp. 157–164). ACM.

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* (pp. 38-47). ACM.

Sundar, S. S., Oeldorf-Hirsch, A., & Garga, A. (2008). "A cognitive-heuristics approach to understanding presence in virtual environments." In A. Spagnolli & L. Gamberini (Eds.), PRESENCE 2008: *Proceedings of the 11th Annual International Workshop on Presence* (pp. 219–228). Padova, Italy: CLEUP Cooperativa Libraria Universitaria Padova.

Sung, E., & Mayer, R. E. (2012). Five facets of social presence in online distance education. *Computers in Human Behavior, 28*(5), 1738-1747.

Thaler, R., & Sunstein, C. (2008). *Nudge: Improving decisions about health, wealth, and happiness.* Yale University Press, New Haven, CT.

Troussard, X., & van Bavel, R. (2018). How can behavioural insights be used to improve EU policy? *Intereconomics, 53*(1), 8-12.

Veltri, G. A., & Ivchenko, A. (2017). The impact of different forms of cognitive scarcity on online privacy disclosure. *Computers in Human Behavior, 73,* 238-246.

Wu, K. W., Huang, S. Y., Yen, D. C. & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889-897.