WISP 2019 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

12-15-2019

Social looks can be deceiving— How social cues affect information disclosure for high-trust users?

Lior Zalmanson

Gal Oestreicher-Singer

Yael Ecker

SOCIAL LOOKS CAN BE DECEIVING – HOW SOCIAL CUES AFFECT INFORMATION DISCLOSURE FOR HIGH-TRUST USERS?

Lior Zalmanson & Gal Oestreicher-Singer
Coller School of Business
Tel Aviv University

Yael Ecker
Social Cognition Center
University of Cologne

ABSTRACT

Across different domains, a growing number of websites are incorporating social features. This study shows that the mere presence of social cues on a website (such as functions for "liking" content or commenting) can cause users who perceive the website as trustworthy to expose themselves to potentially harmful consequences. We carried out an experiment utilizing a YouTube-like video platform that provides the opportunity to study users' behaviors and perceptions in a realistic, controlled environment. Our results show that, among users who were primed to perceive the website as trustworthy (as opposed to untrustworthy), those who were exposed to social features disclosed more personal information compared with users who were not exposed. Moreover, among high-trust participants, the effect of social features on information disclosure was mediated by participants' perception that they can connect to other people on the platform. Moreover, the presence of social cues did not influence participants' privacy concerns.

Keywords: Privacy, Experiments, Information disclosure, Trust, Social cues, Social features

INTRODUCTION AND THEORATICAL FOUNDATIONS

Social interactions are increasingly becoming integral to the internet usage experience. Websites that once offered only basic informational or monetary transactions now give users opportunities to "like" or rate content and to express their views, as well as to share their favorite content, read other people's views, and form social relationships with other users (Bapna and Umyarov 2015, Burtch et al. 2015). It is not difficult to understand why people welcome the opportunity to feel a sense of community instead of a solitary experience of browsing and searching for information. Human beings are, by nature, highly social creatures; they grow and thrive through social interaction (Baumeister & Leary 1995, Reis et al. 2000). And websites, too, benefit when they provide their users with opportunities to fulfill their social needs: Social features encourage users to produce content or to organize existing content in a manner that enhances website usage for themselves and for others and strengthens the website community. Further, compared with passive consumers, users who engage in social participatory actions show greater loyalty and commitment to the website, in addition to higher willingness to pay for the site's services (Bapna and Umyarov 2015, Burtch et al. 2015, Dewan and Ramaprasad 2014, Oestreicher-Singer and Zalmanson 2013).

Herein, we suggest that the benefits inherent to social features on online platforms may conceal a darker side. In particular, people's social tendencies can expose them to risks of identity theft and data breach. It might seem that many of the social features that are common on contemporary websites should not elicit suspicion in this regard; for example, there is nothing particularly revealing about rating a nature video or 'liking' a funny image of a cat. Yet, we suggest that the mere presence of such social features on a website may encourage certain users—specifically, users who generally perceive the website as trustworthy—to become more likely to reveal personal information, and thus to expose themselves to risk.

Research shows users are reportedly worried about the security of their personal data, but they still choose to reveal such data online on many occasions (Angst and Agarwal 2009, Pew Research Center 2014). This discrepancy, which has raised interest in the IS field, is referred to as the *privacy paradox* (Pavlou 2011, Acquisti et al. 2015, Adjerid et al. 2016). One explanation provided for this paradox draws from the idea that, when deciding whether to reveal personal details, users are often in a state of uncertainty and feel that they possess insufficient information to make the decision (Acquisti et al. 2015). Accordingly, a user deciding whether to reveal information to a website might compensate for this insufficiency by searching for environmental cues indicating whether information revelation would be desirable (John et. al. 2011, Acquisti et al. 2015). We contribute to untangling the privacy paradox by pointing to the role of social features as a cue with the potential to enhance information revelation behavior.

Our main premise in the current paper is that the presence of social features on websites is a type of environmental cue that can cause people to behave as they would in a real-life social situation. One important aspect of social behavior is openness and disclosure (Erikson 1963). Consequently, among users who perceive the website as generally trustworthy, the mere presence of social features in the website may lead to an increase in the likelihood of revealing personal information, as it would in a real-life social situation in which an individual feels comfortable. In contrast, when the user does not perceive the website as trustworthy, the mere presence of social features could lead users to withhold information, as in a social situation in which an individual feels uncomfortable. Importantly, we propose that these effects are triggered by the mere presence of social features, regardless of whether the user actually uses them .

Accordingly, we formulate the following hypothesis: *H1. The presence of* ***social cues*** *on a website encourages information revelation online among participants with high trust towards the website, but not among participants with low trust towards the website.*

We note that the capacity to test this hypothesis is limited by the possibility that trust and social cues may not be independent: Specifically, it is possible that the very presence of social cues on a website might strengthen (or weaken) users' trust in that website. We suggest that, given the ubiquity of social features on contemporary websites, users are unlikely to perceive such features as a distinctive characteristic that signals a website's trustworthiness. Nevertheless, this concern is addressed in our empirical analysis.

Our hypothesis regarding the role of social cues in information disclosure (in the presence of trust) relies on the assumption that individuals indeed perceive a website's social features as 'social'—i.e., as an opportunity to connect with others. This perception is necessary in order for these features to activate participants' social goals, though it is important to note that individuals may not be consciously aware of their perception of a website's social aspects as being 'social' (Custers & Aarts 2010; Dijksterhuis, Chartrand, & Aarts 2007). Accordingly, we hypothesize: *H2. Perceptions of* ***being able to connect*** *to others via a website will mediate the relationship between the presence of social cues on the website and the level of personal information disclosure among participants with high trust*.

We base our next hypothesis on the privacy paradox literature, which shows that people generally express stable privacy concerns, though the manner in which they handle their personal information might not align with these stated preferences.

H3. The presence of social cues in a website ***does not*** *affect users' general privacy concerns.*

EXPERIMENTAL DESIGN AND MEASUREMENTS

Experimental Context - The VideoBook Website

We empirically examine our hypotheses in a controlled experimental setting: a YouTube-like video site named VideoBook, described in past work by XXX (Anonymized). The website provides users with sessions in which they can browse various videos, which are displayed on a built-in video player (see Figure 1).

Videos in VideoBook were taken from the Vimeo website. Vimeo.com is one of the largest video websites in the world and specializes in artistic, high-quality videos. By using Vimeo.com as a source (as opposed to YouTube.com, for example), we avoided the risk of encountering an uncontrolled distraction or interruption in the form of an online ad. In order to make sure that the quality of users' experience would not be influenced by the specific videos they chose to watch, the videos to which users were exposed were limited to highly rated high-resolution nature videos. We argue that, compared to music videos or narrative-led video clips, the nature genre is probably less associated with cultural differences and diverse personal tastes. Thus, our selection of videos enabled us to reduce variance resulting from users' personal video preferences.

Methodology

Participants and Design

In this experiment, we tested our hypotheses by manipulating (i) VideoBook users' exposure to social cues on the website. We recruited 389 participants (50% women; Mage = ~30[1]) through the Prolific website, a crowdsourcing platform initiated by researchers at Oxford, UK[2]. All were registered as US residents. Participants completed the studies over the Internet and were paid 1 GBP for their participation. We randomly assigned participants into four conditions in a 2 (social cues: present vs. absent) × 2 ((manipulated) trust: high vs. low) between-subjects design.

[1] To minimize collection of personal information, we did not collect participants' exact age. Instead, participants indicated their age as a 5-year range. To estimate mean age, we used the mid-values of each range.

Procedure All participants first viewed a screen presenting the following introduction to VideoBook: "You are about to participate in a platform for sharing creative video work. This video-sharing platform is called 'VideoBook'".

Next, participants were exposed to the trust manipulation. Specifically, participants in the high-trust condition saw the following message, which was designed to elicit trust: "*Attention: We are using advanced data protection technology to keep our participants' data private, in accordance with the EU's most recent general data protection regulations (GDPR*)". Participants in the low-trust condition saw the following message, designed to elicit distrust: "*Attention: Due to past security breaches, we have recently improved our data protection techniques. If you still encounter any problem or have concerns on this issue, please contact us*".

Participants in the *social-cues-present* condition then read the following instructions: "The website will play videos for you in the center of the screen. Below each video, you will see ratings, tags and comments. You will also see links to 4 related videos on the right side of the main video frame. You are welcome to browse, engage and play with the website as you normally would with other video content websites. Moreover, you may skip videos and not watch them all the way through". The instructions in the *social-cues-absent* condition omitted any information about the social aspects of the website: "The website will play videos for you in the center of the screen. You will see links to 4 related videos on the right side of the main video frame. You are welcome to browse, skip videos and not watch them all the way through".

Participants then proceeded to a video-watching session. The duration of this session was 6 minutes, during which each participant saw a video in the middle of the screen. The participant was able to switch at any time to a new video by choosing between four other video options that appeared to the right of the main video, or by pressing a "pick random video" button that appeared under the main video. Participants were also able to pause the video using a button located under the video. After the 6-minute video-watching session, participants were automatically transferred to a page where they were asked a series of questions distributed across four separate surveys. The measurements derived from these questions are elaborated in the following subsection. Finally, participants were thanked and debriefed.

Measurements

Trust Manipulation Check: We measured participants' perceptions of trust towards VideoBook by asking them to rate, on a scale of 1–7 (1 = not at all; 7 = very much), their agreement with the following statement: "I think VideoBook is a trustworthy website."

Social Cues Manipulation Check: To verify that participants in the social-cues-present condition were aware of the social features present on VideoBook and perceived them as features characterizing a social network, we included the following item, which participants rated on a scale of 1–7 (1 = not at all; 7 = very much): "Videobook is a social network".

Willingness to Disclose Personal Information: To measure participants' willingness to disclose personal information, we presented them with a questionnaire with seven personal questions. We preceded this questionnaire with the following instructions: "We would like to know a few personal details about you to improve our analysis". To avoid the possibility that participants would feel compelled to answer in order to receive payment, we provided the following clarification: "Some of the questions below are voluntary. You can decline to answer by leaving the text box empty and checking the "I'd rather not say" option. Declining to answer these questions will NOT affect your payment". Participants were then asked to state their age, gender, main occupation, city of residence, zip code, birth date, and full name. The first two questions, age and gender, were mandatory; the remaining five were voluntary. Our measure of personal disclosure for each participant was the number of answers he or she provided for the last three questions (zip code, birth date, and full name). The choice of this measure was based on Sweeny's (2000) findings that these three items of information can give away the complete identity of a person in the US.For the latter questions, we recorded only whether a response was given, and not the content of the response[3].

Perceptions of VideoBook as a Website that Facilitates Social Connections with Others ('Social Perceptions')**:** We measured participants' social perceptions by asking them to rate their agreement with the following statement on a scale of 1–7 (1 = not at all; 7 = very much): "I can relate to others through a website like VideoBook – by sharing, liking or commenting."

Privacy Concerns: To measure participants' privacy concerns, we adapted Malhotra et al.'s (2004) Internet Users' Information Privacy Concerns questionnaire into 10 questions about awareness of privacy practices, collection of data online, unauthorized secondary use, improper access, etc. Participants rated their agreement using a 7-point scale. We calculated each participant's privacy concerns score as the average of his or her responses to these 10 items (Cronbach's α = 0.84).

General Attitude Toward VideoBook: To measure participants' general attitudes toward VideoBook, we asked them to respond to the following questions by rating a 7-point scale: "How enjoyable was your experience?" (1 = not enjoyable at all; 7 = very enjoyable); "How likely are you to recommend VideoBook to your friends?" (1 = not likely at all; 7 = very likely); "What is

[3] The reason for the decision not to record participants' responses was to protect their privacy. Because this project is funded by the ERC, it complies with the EU regulations with regard to protection of users' personal information.

your general impression of VideoBook?" (1 = very low; 7 = very high). We calculated each participant's general attitude score as the average of his or responses to the three items (Cronbach's α = 0.94).

Attention Check: To verify that participants were indeed paying attention to the content of the survey items, we included two attention checks throughout the experiment. In one of the checks the participants respond to the following item: "Please mark the answer '3' here." We also implemented an instructional manipulation check (IMC) to further increase the statistical power of the experiment. IMC has previously been used as a strict measure of participant attentiveness and as an attention filter (Oppenheimer et al. 2009, Kittur et al. 2008). In our version of Oppenheimer et al. (2009), the IMC question was "Do you give your personal data online?" and the options were: sometimes, most of the time, never. In a longer block of text that appeared before this question, participants were told that the aim of the following question was to test their attention, and that they would indicate having read this text by skipping the question. Thus, if a participant answered the question, he or she was disqualified as "not paying close attention". In our empirical estimation we verified the results by running the analysis twice. Once only including those users who passed both the strict IMC and the more lenient attention check, and once with those who passed the lenient test but failed the strict IMC in our sample.

Additional Measures. Participants reported their online savviness ("How many hours per day do you spend online?" (responses ranged from 1 hour to 12 hours)) and their video savviness ("How many hours per day do you spend watching online videos?" (1 hour–12 hours)). Then, participants reported whether they had experienced technical problems, whether they had any comments about the study, and whether they had participated in a similar study in the past.

Participants also answered additional questions, which were not relate to the constructs at the focus of this study and were not ultimately included in our analysis.

RESULTS

Data

To enhance the validity of our results, we took strict measures to ensure the quality of our participants' input. Thus, of the 389 participants recruited for this study, we excluded users for the following reasons (some participants were excluded for multiple reasons): users who experienced technical errors, users who were idle for more than two thirds of their time on the website and were suspected to be 'away from keyboard'; participants who watched two segments or fewer of the two minute videos or more than 14 segments of two-minute videos over the duration of the 6-minute session, as this behavior hinted that users were not focused on content consumption; participants who indicated that they had participated in a similar study in the past; and participants who failed our attention checks (see details in the "Measurements" subsection of our description of the experimental design of Experiment A above). Ultimately, 208 participants entered the analysis (54% women; average age ~30)[4].

Manipulation Checks: Trust and Social Cues Manipulations

A *t*-test on perceptions of trust found a significant effect of trust condition, *t*(1, 204) =-2.067, *p* = .040, such that participants in the high-trust condition indeed expressed greater trust in VideoBook (*M* = 4.68, *SD* = 1.33) compared with participants in the low-trust condition (*M* = 4.29, *SD* = 1.37). For our social cues manipulation check, a *t*-test found that participants in the

[4] We acknowledge that the final sample is substantially smaller than our originally recruited sample; we note, however, that these numbers (and even lower percentages) were documented among populations recruited from online subject pools and who was administered the instructional manipulation check (Hauser and Schwartz 2015).

social-cues-present condition were significantly more likely than participants in the social-cues-absent condition to perceive VideoBook as a social network, 4.06 vs. 2.99 on the Likert scale, $t(1, 205) = -4.856$, $p < .001$.

H1: The Role of Trust and Social Cues in Disclosure of Personal Information

H1 predicts that the presence of social cues on a website should encourage information disclosure among participants with high trust towards the website, but not among participants with low trust towards the website. To address H1, for each trust condition, we used a t-test to compare participants in the social-cues-present condition with those in the social-cues-absent condition. For participants in the high-trust condition, social cues condition had a significant effect on information disclosure, t(110.932) = -2.182, p < .05, such that participants in the social-cues-present condition disclosed 2.1 personal information items (STD = 0.886), whereas participants in the social-cues-absent condition revealed only 1.68 items (STD = 1.14). In contrast, among participants in the low-trust condition, we observed no relationship between social cues condition and information disclosure (1.68 [STD=1.01] vs. 1.69 [STD=1.06] items without and with social cues respectively, p = .992). Taken together, the findings support H1[5].

H2: The Role of Social Perceptions in the Relationship between Trust, Social Cues, and Information Disclosure

As expected, for each trust condition, participants in the social-cues-present condition had higher social perception scores than did participants in the social-cues-absent condition, $F(1, 110) = -2.39$, $p < .05$ (see Table 1). To test H2, for participants in the high-trust condition, we conducted a mediation analysis using R's Lavaan package (version 0.5-16; Rosseel, 2012), to

[5] For robustness, we also ran all the analyses including people who did not pass the strict attention check and found similar patterns.

examine whether social perceptions (i.e., the perception that one can connect to others on VideoBook) mediated the effect of social cues condition on information disclosure. We used the bootstrap method to estimate confidence intervals for the effects. The mediation analysis indeed revealed a significant indirect effect, $B = .143$, $Z = 2.66$, $p = .008$, of social cues condition on information disclosure, through social perceptions; this result supports H2. We note that the direct effect in that analysis was not significant, $B = -.16$, $Z = -1.45$, $p = .146$, meaning a full mediation in which information disclosure for high trust users can be explained by their social perceptions.

H3: Privacy Concerns

Table 2 presents mean privacy concerns scores by experimental condition. A 2×2 ANOVA found no differences in privacy concerns between the experimental conditions, $p > .185$, supporting H3. Overall all three hypotheses were supported in Experiment A.

Addressing Alternative Explanations

Individual Characteristics : Table 3 presents participants' individual characteristics by experimental condition. Though the distribution of participants across conditions was random, there might nevertheless have been differences between experimental conditions that biased our results. To refute this possibility, we conducted 2 (social cues: present vs. absent) × 2 (trust: high vs. low) ANOVAs on age, online savviness, and video savviness. (Given that participants indicated their age range rather than their exact age, we estimated each participant's exact age as the middle point of his or her age range.) There were no significant differences in participants' age, online or video savviness between experimental conditions (ps > 0.5). Finally, a logistic regression analysis found no significant differences in the ratios of men and women between experimental conditions.

General Attitudes toward VideoBook: Table 4 presents participants' ratings regarding their general attitudes toward VideoBook. A 2 (social cues: present vs. absent) × 2 (trust: high vs. low) ANOVA on the general attitude score found no difference between the experimental conditions (all items p > .25).

Activity on the Website: In the social-cues-present condition, participants were able to rate, like, and comment freely on the videos, and they indeed used these features: On average, participants in this condition rated the video 1.6 times during the video session, liked/disliked the videos 1.03 times, and commented on the videos 0.42 times. Table 5 presents disclosure scores by experimental condition, level of trust, and a binary variable indicating whether the participant used a social feature at least once. Considering only participants in the high-trust condition who were exposed to social cues, participants who participated at least once were not significantly more willing to disclose personal information compared with those who did not participate at all (p = 0.321). Moreover, among high-trust participants, both the active and the inactive participants in the social-cues-present condition disclosed more personal information than did (high-trust) participants in the social-cues-absent condition. These results show that the presence of social cues rather than actual social participation is what drives the effect on information disclosure.

Trust Manipulation vs. Measured Trust: To further assess that the effectiveness of the trust manipulation was not likely to have been influenced by participants' assignment to social cues conditions, we ran an additional experiment. However, in this case, participants proceeded directly to the video-watching session instead of undergoing a trust manipulation. Overall, 163 participants entered the analysis (49% women, Mage = 30.73, SDage = 10.56). Specifically, 71 participants entered the social-cues-present condition, whereas 92 entered the social-cues-absent condition. Users' mean level of trust in the website was 4.76, with a median score of 5. A t-test showed that the trust levels of participants in the social-cues-present condition (M = 4.77, SD = 1.14) did not differ significantly from the trust levels of participants in the social-cues-absent condition (M = 4.75, SD = 1.47; t(161) = 0.12, p = .90). This observation suggests that exposure to social cues did not affect participants' perceptions of VideoBook's trustworthiness.

DISCUSSION AND CONCLUSIONS

Our analyses show that an individual's trust in a website interacts with the presence of social features on that site to influence his or her willingness to disclose personal information. Specifically, our results lend support to the idea that when participants perceive a website as trustworthy, exposure to social cues (in the form of features such as the possibility to like, rate, and comment on videos) causes them to disclose more personal information than they do when such features are absent (H1). We also found that, among high-trust participants, the influence of social cues on personal disclosure was mediated by the extent to which participants believed that they could connect to other people on the website (H2). Finally, the presence of social cues did not affect participants' privacy concerns (H3).

Our findings carry several theoretical implications and contributions. First, though information privacy research has explored the discrepancies between information revelation and privacy concerns (Aqcuisti and Gross 2006), and the connection between trust and information revelation (Smith et al. 2012), to our knowledge, our work is the first to explore how information revelation is influenced by the presence of online social features. Our observations suggest that, when using social networks, high-trust individuals may be especially vulnerable to harmful consequences such as spam, identity theft, bullying, and extortion, owing to their heightened propensity to disclose personal information in the presence of social features. We further contribute to research on the development of trust in websites. Past work has shown that a user's level of trust in a website is a function of familiarity and past experience with the website, which develops over time (Gefen 2000). In our work, we observed that users were able to develop a sense of trust in the website in mere minutes—and that it was possible to manipulate this sense of trust to some degree through the use of a message.

Finally, our findings contribute to research on the privacy paradox (Pavlou 2011; Acquisti et al. 2015), in showing that the presence of social cues did not affect general concerns about privacy, though it did affect information revelation behavior. One explanation that has been proposed is that "one might care deeply about privacy in general but, depending on the costs and benefits prevailing in a specific situation, seek or not seek privacy protection" (Acquisti et al. 2015, p. 510). Our findings support this idea, suggesting that information revelation decisions can be manipulated, whereas general privacy concerns are much more stable.

Our findings also carry several managerial and policy implications. We show that the social features of online platforms may serve as a powerful tool for manipulation of information disclosure. Whereas the risks of information disclosure are well acknowledged, the presence of social features, such as the ability to rate, like, and comment on videos, are not known to be associated with harmful effects. If online social features and information disclosure are, in fact, intertwined, the possible harm associated with the social aspects of the internet should be brought to the attention of policy makers and the public in general.

Our work is not without limitations. The randomized experimental settings and the manner in which they were designed enabled us to control for different effects, as well as to test for causation. However, one might claim that the laboratory setting is also a limitation of the research. Other limitations include the fact that our findings may be specific to environments resembling VideoBook (a YouTube-like website). Furthermore, for the participants in our experiment, VideoBook was an unfamiliar website, which they were using for the first time. Testing the effects of social cues in a well-known environment with established trust perceptions might yield different results. These questions present interesting avenues for future work.

REFERENCES

Acquisti, A. and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Lecture Notes in Computer Science* (42:58), pp.36-58.

Acquisti, A. and Grossklags, J. 2012. "An Online Survey Experiment on Ambiguity and Privacy," *Digiworld Economic Journal* (88:4), pp.19-39

Acquisti, A., Brandimarte, L. and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information," *Science* (347:6221), pp.509-514.

Adjerid, I., Peer, E. and Acquisti, A. 2018. "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," *Management Information Systems Quarterly*, (42:2), pp.465-488.

Bapna, R. and Umyarov, A. 2015. “Do your Online Friends Make You Pay? A Randomized Field Experiment on Peer Influence in Online Social Networks,” *Management Science* (61:8), pp.1902-1920.

Baumeister, R. F and Leary, M. R. 2017. “The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation,” in *Interpersonal Development* Routledge pp. 57-89.

Burtch, G., Hong, Y., Bapna, R. and, Griskevicius, V. 2015. "What Are Social Incentives Worth? A Randomized Field Experiment in User Content Generation," *International Conference on Information Systems*.

Custers, R. and Aarts, H. 2010. The Unconscious Will: How the Pursuit of Goals Operates Outside of Conscious Awareness,” *Science*, (329:5987), pp. 47-50.

Dewan, S. and Ramaprasad, J. 2012. “Research Note-Music Blogging, Online Sampling, and the Long Tail,” *Information Systems Research*, (23:3), pp.1056-1067

Dijksterhuis, A., Chartrand, T. L. and Aarts, H. 2007. “Effects of Priming and Perception on Social Behavior and Goal Pursuit,” In J. A. Bargh (Ed.), *Frontiers of Social Psychology. Social Psychology and the Unconscious: The Automaticity of Higher Mental Processes*, New York, NY, US: Psychology Press, pp. 51-131.

Erikson, E. H. 1963. *Childhood and Society*, 2nd ed., Norton, New York.

Gefen, D. 2000. “E-commerce: The Role of Familiarity and Trust,” Omega (28:6), pp. 725–737.

Hauser, D.J. and Schwarz, N. 2016. “Attentive Turkers: MTurk Participants Perform Better on Online Attention Checks than do Subject Pool Participants,” *Behavior research methods* (48:1), pp. 400-407.

Kittur, A., Chi, E.H. and Suh, B. 2008. “Crowdsourcing User Studies with Mechanical Turk. In *Proceedings of the SIGCHI conference on human factors in computing systems.* pp. 453-456.

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

Oestreicher-Singer, G. and Zalmanson, L. 2013. “Content or Community? A Digital Business Strategy for Content Providers in the Social Age,” *MIS Quarterly* (37:2), pp.591-616

Oppenheimer, D.M., Meyvis, T. and Davidenko, N., 2009. “Instructional Manipulation Checks: Detecting Satisficing to Increase Statistical Power,” *Journal of experimental social psychology*, (*45*:4), pp. 867-872.

Pavlou, P. A. 2003. “Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model,” *International Journal of Electronic* Commerce (7:3), pp.69-103

Pavlou, P. A. 2011. “State of the Information Privacy Literature: Where are We Now and Where Should We Go?” *MIS Quarterly* (35:4), pp. 977-988

Pavlou, P. and Gefen D. 2004. “Building Effective Online Marketplaces with Institution-Based Trust,” *Information Systems Research* (15:1), pp. 37–59.

Pew Research Center, *Internet, Science and Tech*. 2014. The Internet Project.

Reis, H. T., Sheldon, K. M., Gable, S. L., Roscoe, J. and Ryan, R. M. 2000. “Daily Well-Being: The Role of Autonomy, Competence, and Relatedness,” *Personality and Social Psychology Bulletin* (26:4), pp. 419-435.

Shin, W., and. Kang, H. 2016. “Adolescents' Privacy Concerns and Information Disclosure Online: The Role of Parents and the Internet,” *Computers in Human Behavior* (54), pp.114-123

Zalmanson, L., and Oestreicher-Singer, G. 2015. “Your Action is Needed: The Effect of Website-Initiated Participation on User Contributions to Content Websites,” *International Conference on Information Systems 2015.*

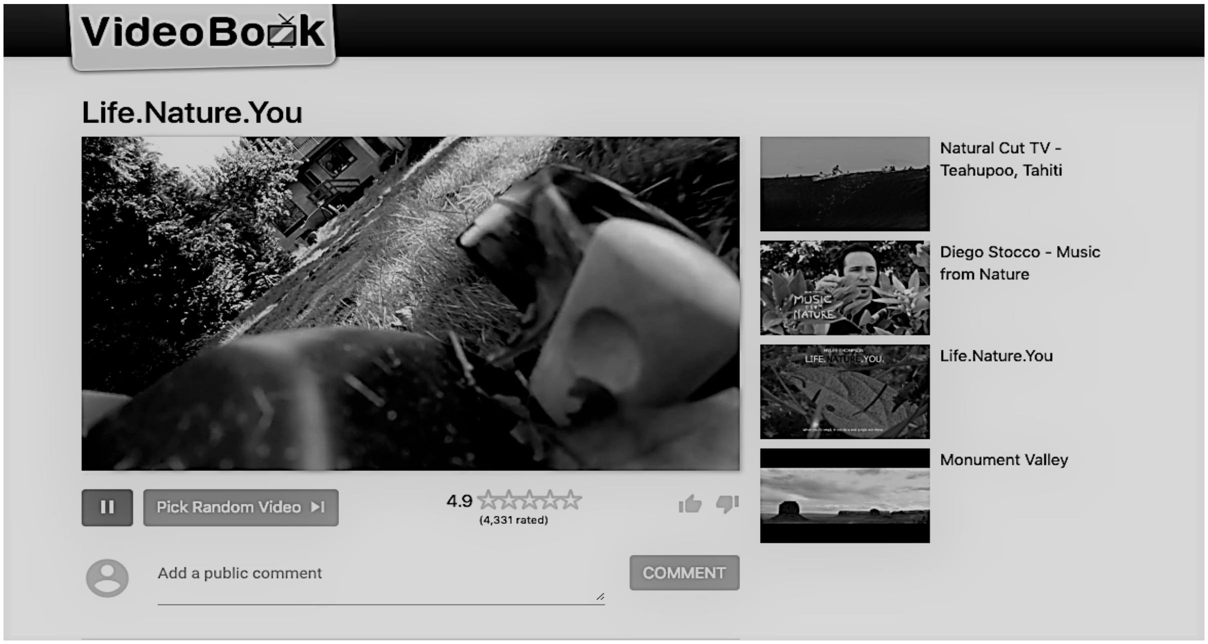

Figure 1. The VideoBook screen with social cues (social-cues-present conditions).

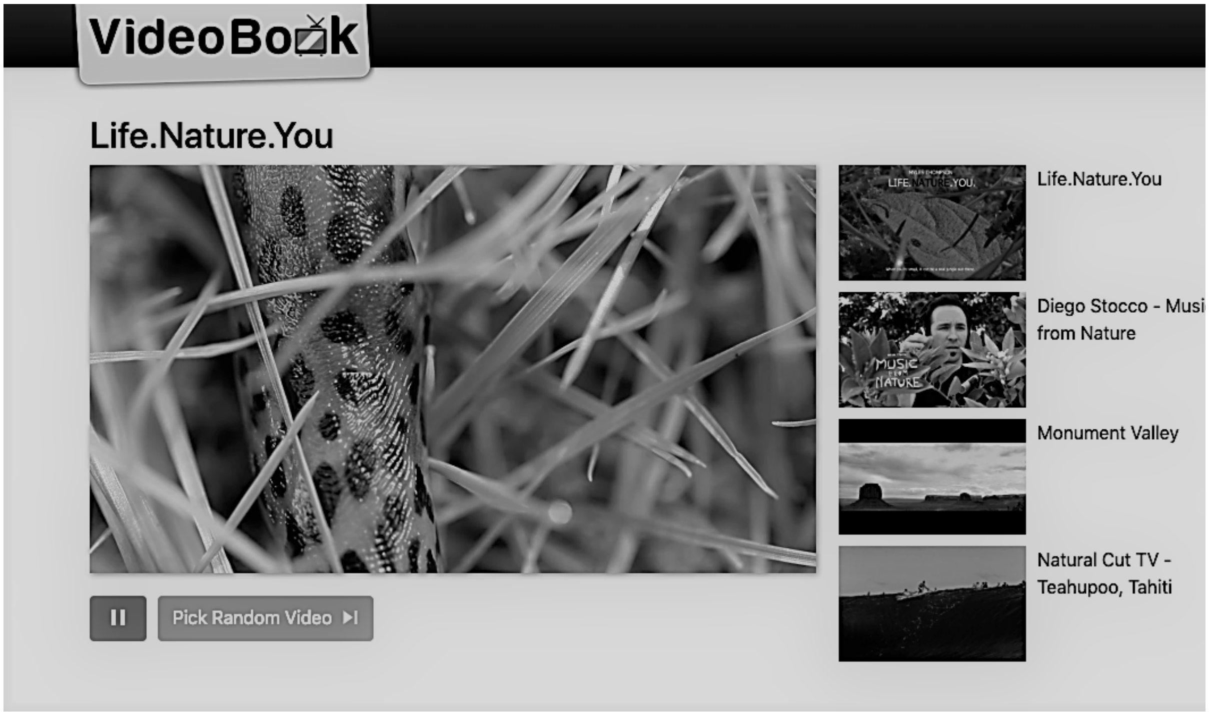

Figure 2. The VideoBook screen in the social-cues-absent condition.

Table 1.

Participants' perceptions of VideoBook as a social website

	Trust condition:	
Social cues condition:	*Low*	*High*
I can relate to others through a website like VideoBook – by sharing, liking or commenting.		
Social cues present	4.69 (1.56)	4.78 (1.63)
Social cues absent	3.48 (1.87)	4.08 (1.50)

Notes. All measures are on a scale ranging from 1 to 7.

Table 2.

Mean privacy concerns scores by experimental condition (standard deviations in parentheses)

	Trust condition	
Social cues condition	**Low**	**High**
Social cues present	6.08 (.73)	5.91 (0.63)
Social cues absent	5.92 (0.89)	6.02 (0.71)

Notes. Responses to the privacy concerns items were on a 7-point scale.

Table 3.

Demographic variables by experimental condition (standard deviations in parentheses).

	Trust manipulation:	
Social cues manipulation:	**Low**	**High**
Age:		
Social cues present	31.11 (12.86)	29.00 (9.50)
Social cues absent	30.60 (10.45)	29.65 (9.21)
Gender:		

Social cues present	0.52 (0.50)	0.52 (0.50)
Social cues absent	0.51 (0.51)	0.59 (0.50)
How many hours a day do you spend online? (number of hours).		
Social cues present	4.78(2.53)	4.61 (2.74)
Social cues absent	5.02 (2.00)	4.70 (2.56)
How many hours a day do you spend watching online videos? (number of hours).		
Social cues present	2.44 (1.86)	2.31 (1.43)
Social cues absent	2.22 (1.52)	2.52 (1.93)

Notes. Gender is the proportion of females in the sample. Age was collected in ranges and calculated here using the mid-point of each range, which helps explain the high standard deviation. Online savviness and video savviness were measured on a 12-point scale (1= up to one hour, 12 = 12 hours or more).

Table 4.

Mean ratings on general attitude questions about VideoBook by experimental condition.

	Trust condition:	
Social cues condition:	**Low**	**High**
How enjoyable was your experience?		
Social cues present	4.24 (1.83)	4.52 (1.56)

Social cues absent	3.93 (1.68)	4.32 (1.62)
How likely are you to recommend VideoBook to your friends?		
Social cues present	4.65 (1.74)	4.61 (1.53)
Social cues absent	4.27 (1.53)	4.65 (1.54)
What is your general impression of VideoBook?		
Social cues present	3.65 (2.15)	3.80 (2.03)
Social cues absent	3.31 (1.82)	3.55 (1.82)

Notes. All measures are on a scale ranging from 1 to 7.

Table 5.

Mean disclosure of personal information scores by experimental condition and level of trust (Standard deviations in parentheses).

Experimental conditions:	**Level of trust:**	**Participated:**	
Social cues present	High	Yes	2.20 (0.773)

		No	1.95 (1.02)
	Low	Yes	1.61 (0.99)
		No	1.83 (1.20)
Social cues absent	High	—	1.68 (1.14)
	Low	—	1.68 (1.01)

Notes. Disclosure scores are calculated as the number of personal details that participants provided, ranging from 0 to 3.