Optimizing Privacy Policy Videos to Mitigate the Privacy Policy Paradox

Mark J. Keith
Brigham Young University
mark.keith@gmail.com

Jacob T. Fredericksen
Brigham Young University
jacob.t.fredericksen@gmail.com

K. Shane Reeves
Brigham Young University
kshanereeves@gmail.com

Jeffry Babb
West Texas A&M University
jbabb@wtamu.edu

Abstract

This research takes a design science approach to improving privacy policies through the design and use of mediated content, such as video. Research has emerged to indicate that privacy policies communicated through video (separate from—and in addition to—traditional textual privacy policy documents) are more effective at engendering trust, decreasing perceived risk, and encouraging information disclosure than textual privacy policies, which are seldom read or understood. We extend this research by examining design factors such as narrator gender, animation style, music tone, and color scheme. We implemented a field experiment and survey to determine how variations in these design elements affect consumers' perceived risk, perceived benefits, and disclosure decisions. The results indicate that the most effective privacy policy videos use female narrators with vibrant color palettes and light musical tones. The animation style (animated imagery versus animated text) has no effect on consumers' perceived risk/benefits or disclosure decisions.

1. Introduction

Information privacy research has largely focused on understanding why consumers, who are assumed to be "rational," choose to disclose so much personal information during consumer-provider interactions such as website registrations, transactions, mobile app installations, etc. in return for seemingly small benefits, contrary to the fact that these consumers claim to have significant privacy concerns [7, 61]; this phenomenon (in which consumers' disclosure behavior does not match their disclosure intentions) is known as the "privacy paradox" [48]. However, more recent research has argued that consumers cannot be fully rational decision makers because they do not know the data-related intentions or practices of the provider (of the goods or services, esp. software, for which consumers data is collected) [1, 2, 28, 32, 63] and therefore cannot evaluate true privacy risk.

In order to reduce information asymmetry between consumers and providers of data-based personalization services, privacy regulators—including government bodies [12, 14, 13, 58, 46] and mobile app platforms [5]—require that providers disclose their data practices through "privacy policies" [66]. However, research indicates that privacy policies are ineffective and troublesome because (1) they typically are not read or are too difficult for consumers to understand [21, 43, 55] and (2) they may have the unintended effect of *raising* consumer privacy concerns rather than reducing them [55]. The first problem arises because consumers, regulators, and producers have different motivations in (respectively) reading, regulating, and designing privacy policies. Generally, consumers want to be assured that their personal data will be protected, but they also want a seamless experience and have little desire to expend the effort to read lengthy, legalistic documents. Regulators are interested in safeguarding consumers (by ensuring that consumers are provided with comprehensive information regarding producers' data practices) while enabling producers. Producers are interested in fulfilling two competing objectives: (1) providing comprehensive information regarding their data practices to stay ahead of legal or regulatory action and (2) assuring and building trust with consumers to encourage information disclosure.

We have termed the difficulty experienced by producers in fulfilling both objectives within a single privacy policy as the "privacy *policy* paradox" [30]. Consumers benefit (in terms of ability to make rational decisions) from easy-to-read, easy-to-understand privacy policies, which reduce information asymmetry between them and producers. However, given that any noticeable privacy policy may heighten consumer privacy concerns and reduce information disclosure [35, 30], producers are motivated primarily to fulfill the first objective—complying with regulations and protecting themselves against privacy-related lawsuits—rather than to create highly "consumable" privacy policies that effectively fulfill the second objective (i.e., assuring consumers and building trust). The frequent result is privacy policies that cost more (in terms of effort required to read) than they are worth (in terms of benefits from reading) to consumers.

URI: http://hdl.handle.net/10125/50355
ISBN: 978-0-9981331-1-9

Accordingly, consumers often ignore privacy policies and instead use heuristics such as mobile app ratings, number of downloads, brand credibility, and privacy seals (which do not actually communicate providers' practices) [27, 37] to inform their information disclosure decisions.

To resolve this problem, some regulators (e.g., European Union [12]) and researchers [30] have suggested using "layered" privacy policies in which a summary version is presented to consumers along with access to more detailed information and/or the full document (separate from the summary version). Prior research has provided suggestions for optimizing the content of the summarized, "consumable" version and has suggested that this version is better implemented as a short, understandable, commercial-like video than as a textual statement [35, 30]. However, while video has shown remarkable promise in initial tests as a medium for communicating summarized privacy policies, the research is still in its infancy and does not provide clear direction regarding how to optimize the *delivery* of privacy policy content (rather than the content itself) to increase consumer attention, understanding, trust in the provider, favorable perceptions of information disclosure risks/benefits, and actual information disclosure. Accordingly, the objective of this research is to identify optimal design characteristics (i.e., design characteristics that maximize these constructs) of privacy policy videos. In so doing, we do not aim to "take the side" of consumers, providers, or regulators. Rather, we attempt to demonstrate transparently how the delivery of privacy policy content affects consumers' perceptions and behaviors. Providers may use the results of this research to attempt to minimize consumers' perceived risk, while regulators may use the results to establish privacy policy requirements or restrictions.

For purposes of this research, we take a design science approach, in which design elements are theory-driven and the ultimate theoretical contribution is in the design of the artifact [24, 22, 39, 52]. First, we created a mobile app that requests and uses a variety of sensitive consumer data. We next hired a professional video producer with extensive experience in commercial production (esp. animation) to generate 24 unique versions of the same privacy policy script. These versions varied based on four factors known to have an impact on consumers' psychological perceptions: gender of narrator voice (male versus female), tone of background music (no music, light tone, dark tone), palette of colors used to animate the video (vibrant versus "corporate"), and nature of the animation itself (text-based versus imagery-based). We integrated the commercial-like privacy policy video into the initial usage of the app so that consumers were forced to view it before they could proceed with app testing and registration. Each consumer who used the app was randomly assigned one of the 24 versions of the privacy policy. Effects of the videos were thus tested "in context" (as they would be in actual practice) rather than in an artificial laboratory environment.

2. Theory and Literature

2.1. Why Privacy Policy Videos?

The proposition that videos may be more effective than privacy policy documents as a means of reducing consumer privacy fears and engendering trust is supported both by theory and by research findings.

Theoretical support centers on the richer visual rhetoric conveyed by video and on the combination of visual information with auditory information. Videos present visual metaphors, which help with understanding new phenomena and classifying encountered phenomena into a known or familiar context [53]; this is a key component of learning [33]. Furthermore, video incorporates human voice, which, according to theory on multimedia, influences human behavior by carrying important nonlinguistic signals or cues [8]. The *cognitive theory of multimedia learning* [40] posits that because humans process visual information and auditory information separately and simultaneously in "dual channels," each of which is limited in the amount of information that can be processed at one time, humans are able to learn more meaningfully and lastingly from a combination of visual and auditory information than from only one or the other [41]. Privacy policy videos that are designed to minimize cognitive overload [42] and encourage active learning [40] are therefore more likely than textual privacy policies to reduce information asymmetry between providers and consumers.

Perhaps most importantly, two studies have confirmed that privacy policies, which are intended to build trust, minimize perceived risk, and encourage information disclosure, have that exact effect more strongly when presented through videos rather than text [35, 30]. Accordingly, we proceed by reviewing theory to argue which video design elements will most pronounce this effect.

2.2. Theoretical Video Design Elements

The use of video (rather than textual documents) to communicate privacy policies to consumers introduces new design variables by which consumers' risk/benefit perceptions and disclosure behavior may be impacted. Relevant factors include animation style [36, 9], color palette [36, 20], background music [60, 25] and narrator's gender [64, 10, 65]. As we are testing the constructs, models, methods, and instantiations of mediated content for privacy policy design, we facilitated design evaluation via hypothesis testing [39] by implementing the predicted optimal and suboptimal variations of all factors. Hypotheses regarding design factors are found below.

2.2.1. Animation. Privacy policy videos can be animated using imagery relevant to product functionality and data practices or using "redundant presentation," in which content is simultaneously presented through narration and as on-screen text. Research indicates that redundant presentation may increase cognitive overload in viewers by causing viewers to "devote cognitive capacity to processing the on-screen text and reconciling it with the narration" [42]. In an educational context, non-redundant multimedia presentations were demonstrated to help students more than redundant presentations to learn [42]. Based on this redundancy effect, we expect that animated images will help consumers to learn about producers' data practices better than will text-based animation. We expect that by so doing, image-based animation will reduce perceived information asymmetry and thereby decrease perceived risk, increase trust, and increase information disclosure.

> *H1: Fully animated imagery will have a greater effect on decreasing perceived risk and increasing trust, perceived benefits, information disclosure than text-based animation.*

2.2.2. Color Palette. Marketing research indicates that colors of a higher "value" (i.e., brighter colors) in ads cause consumers to feel more relaxed and to like ads better (as compared to lower-value colors) [20]. Similarly, consumers exhibit a "visual saliency bias" in which they are more likely to select products with brighter packaging and, interestingly, that this bias becomes stronger when consumers are placed under conditions of greater cognitive load [45]. Because the privacy policy context involves relatively high-cognitive-load conditions, we expect a pronounced, similar effect in which more vibrant color palettes in privacy policy videos will lead to less attention paid to privacy risks resulting in more information disclosure than "corporate" color palettes.

> *H2: Vibrant color palettes will have a greater effect on decreasing perceived risk and increasing trust, perceived benefits, information disclosure than "corporate" color palettes.*

2.2.3. Music Tone. Research indicates that music is an affective background component that causes consumers to feel a sense of attachment to a product independent of cognitive processes [60] and that music acts as a symbol of meaning and therefore affects consumers' interpretation of meaning in advertisements [25]. Based on these findings, we expect that privacy policies with background music that is light in tone will decrease perceived risk, increase trust, increase perceived benefits, and increase information disclosure as compared to music that is dark in tone or no music.

> *H3: Music with a lighter tone will decrease perceived risk and increase trust, perceived benefits, and information disclosure relative to no music or to music with a darker tone.*

2.2.4. Narrator Gender. Research regarding the impact of gender on trust is mixed. Some studies have indicated that women are trusted more than men [65]. Although a study using the Investment Game to examine gender and trust found that females are more trust*worthy* than men but that neither gender is trusted more than the other and gender effects on other variables (not trust) vary by context [64], we expect that in the privacy policy context, female narrators will be perceived more favorably than male narrators.

> *H4: Female voices will decrease perceived risk and increase trust, perceived benefits, and information disclosure compared to male voices.*

3. Evaluation

To test our video privacy policy design, we needed to select a privacy policy context. We could not test the privacy policy videos in a disaffected laboratory environment because participants would know that there is no real privacy risk. Rather, so that participants could experience the privacy policy in a natural environment, we began by selecting the mobile app context. We deemed this appropriate because today's mobile app technology allows for unprecedented combinations of consumer data in ubiquitous devices [3, 6, 26, 29, 67], thus maximizing information privacy risk exposure. We developed a hypothetical mobile app, called "Sharing Tree," that is intended to collect a consumer's personal demographic data, GPS location data, social network data (by logging into Facebook, Instagram, etc), and financial data for automating purchases. Sharing Tree uses this data to generate "intelligent finds" (i.e. predicted based on statistical algorithms) for the consumer and their friends. For example, based on your data, Sharing Tree predicts activities (concerts, dining, entertainment) that you would enjoy as well as the specific group of social network contacts (friends and family members) who are likely to want to join you in those activities.

After creating the hypothetical scenario, we developed the app using HTML5 (to make it platform independent) so that it could be tested out on any device. We developed just enough of the app to allow its features to be tested in "alpha" mode, meaning participants could navigate to the app, login under a test account, and view the features for that test account. In addition, participants could use a "Registration" feature and see the many forms of data that would be required or optional to make the app as personalized and useful as possible.

Next, we wrote a script for a simple, condensed version of a privacy policy. Based on the suggestions of regulators (e.g. European Union [12]) and prior researchers [30], this was not meant to be a comprehensive privacy policy that meets all of the regulations of law or mobile app platform rules. Rather, this is meant to be the top layer of a "layered" policy—separate from the full version, shorter, and more likely to be consumed by the user.

Based on suggestions from prior research [30], this policy script included an introduction to the app, a description of *what* data would be collected, *how* the data would be used by the app and provider, and *who* the data would eventually be shared with. To eliminate spurious effects related to the specific content of the privacy policy, which prior research has demonstrated to have a significant impact on risk and trust perceptions [30, 4, 17, 19, 44, 50, 62, 66, 27], we created nine versions of this script with varying levels of content. For example, some scripts only included *what* information would be collected, while others included *how* and *who*. Some scripts specified a realistic list of information to be collected, whereas others specified collection of data that did not appear to "fit" the app's functionality requirements (e.g. camera data was included even though there was no specified need for using the camera in the app). Some scripts stated that the data would be shared with nobody, while others stated that the data would be shared with "partners." Table 1 (below) summarizes each of these nine scripts.

Table 1. Summary of Content Manipulations

1. **Introduce** the app only; no privacy policy content	2. Intro, ***What* (fit)**	4. Intro, *What* (fit), ***How***	6. Intro, What (fit), How, **Who (nobody)**	8. Intro, What (fit), How, **Who (partners)**
	3. Intro, ***What* (misfit)**	5. Intro, *What* (misfit), ***How***	7. Intro, What (misfit), How, **Who (nobody)**	9. Intro, What (misfit), How, **Who (partners)**

To be clear, the primary purpose of this research is not to test or examine how these variations in script content will affect consumer information disclosure, as a complete analysis of the effects of these nine scripts' content is found in prior research [30]. Rather, we implemented these treatments as a control by randomly assigning every eventual participant to one of the treatments so that we would avoid "overfitting" to any particular level and type of privacy policy content. Furthermore, we include control variables representing these nine scripts in our hypothesis testing later. However, the focus of this study is H1-H4: the design factors (beyond privacy policy video content) that affect consumer behavior.

Next, we hired a professional commercial video producer with special expertise in animation-based videos. We allowed the production team to view and try out the Sharing Tree app to better understand it. They then produced a video for each of the nine scripts. In addition, a version of each script was reproduced with (1) male and female narrator voice; (2) imagery-based animation and text-based animation; (3) vibrant colors and muted, "corporate" colors; and (4) no background music, "light"-toned background music, and "dark"-toned background music. In other words, we produced enough versions of the privacy policy for a between-subjects 2 x 2 x 2 x 3 (24 treatments) design. Each of these 24 videos was replicated across all nine versions of the script for a total of 216 unique videos[1].

3.1. Evaluation Procedures

To test our privacy policy video design, we implemented our procedures using a Qualtrics survey with YouTube videos and the Sharing Tree app's HTML embedded. We recruited participants under the false premise (with IRB approval) that they were being recruited to help "consumer focus test" a forthcoming mobile app for an undisclosed (to avoid brand recognition and credibility bias) mobile app development company. Their first task was to watch a "commercial" describing the mobile app. We were

[1] A sample of one of these videos (with a female narrator, dark music tone, full imagery animation, and vibrant color palette) can be viewed at https://www.youtube.com/watch?v=tZ_JxxjyoOs

careful not to describe it as a “privacy policy,” knowing that this could heighten privacy concern [55].

Next, participants were informed that as another form of compensation for their help (in addition to the monetary payment they received for participating), they would be allowed to register to use the app for free for life if they so desired. They were navigated to a registration screen with a variety of mandatory (if they chose to register) information (e.g. email and password) as well as a long list of optional information (address, phone, work history, education, birthday, relationship status, annual income, gender, ethnicity) that would be used to help improve their predictions. The percent of this information that the participant chose to disclose is the primary dependent variable of our analysis. Since we explicitly stated that registration was not required for participants to receive their full payment, we do not suspect that a significant amount of information was falsified.

Finally, participants were navigated to a survey through which we measured several latent constructs to evaluate a variance model explaining consumer information disclosure. This survey concluded the procedures.

3.1.1. Evaluation Participants. To help us evaluate our video privacy policy design factors, we recruited 1,165 participants who completed the entire procedures. Of these, 59 percent were “master” level workers from Amazon Mechanical Turk (AMT) which have been demonstrated to be at least as valid as professionally collected samples [11, 51]. The other 41 percent were students in an introduction to information systems course in the business school of a large western university in the United States. Of those who chose to disclose, 38 percent were female, the average age was 25.8, 82.6 percent were Caucasian, 7.9 percent were Asian/Pacific Islander, 4.5 percent were Hispanic, 3.3 percent were African American, and 1.6 percent Other.

3.2. Evaluation Criteria

To evaluate the effectiveness of each design factor, our survey measured the relevant variables of *privacy calculus* [15, 34], which is the dominant theory used by researchers to explain consumer information disclosure intentions and which has since been modified to be based on actual information disclosure [31] because of the limited relationship between disclosure intentions and behaviors [48].

Privacy calculus posits that consumer information disclosure is based on the rational tradeoff between the consumer’s perceived risk and benefit of disclosing information. Trust in the provider and general privacy concerns are covariates in this model.

Lastly, we measured the construct of *privacy assurance*, which has been modeled as the degree to which the consumer believes that information asymmetry between them and provider has been reduced [30]. Although the relationships among these variables are typically examined in a variance path model, our purpose is not to test privacy calculus or build onto the theory. Rather, we only measure these constructs as endogenous variables that are influenced by privacy policy design factors.

Our measures for privacy assurance (PA), perceived risk (PR), perceived benefits (PB), trust (TRU), and privacy concern (PC) were all drawn from prior research [68, 31, 37]. However, as stated previously, the dependent variable was measured separately as the percent of information disclosed. One final control variable that was measured and that is extremely relevant to our context is the degree to which the participant recalled and paid attention to the privacy policy. We used the following two items: *I paid close attention as I watched the app commercial* and *I only skimmed the information presented in the app commercial*.

By measuring the dependent variable differently from the independent variable, we eliminate the concern of common methods bias [54]. However, the latent reflective constructs are still subject to validation of reliability, convergent validity, discriminant validity, and multi-collinearity. All AVEs were well-over the 0.50 recommended cutoff [18], and all alphas were above the 0.70 cutoff [59], indicating adequate convergent validity. Concerning discriminant validity, the average variance explained (AVE) by the indicators for their underlying latent constructs is greater than the squared correlation between the focal construct and the sub-constructs [18], indicating satisfactory results. Because multicollinearity has been identified as a problem in prior research, we also calculated variance inflation factors (VIF), which were all below the stringent 4.0 cutoff [49].

3.3. Evaluation Results

To further validate our latent factors and actual consumer disclosure variable, we tested them in a structural equation path model using SmartPLS 3.0[2]

[2] PLS-based SEM is appropriate because the constructs *perceived benefits* and *privacy concern* are both second-order formative [18].

[57]. Figure 1 depicts the results. Bootstrapping with 1000 samples was used to generate p-values (*** p < 0.001, ** p < 0.01, * p < 0.05, † p < 0.10). All expected relationships were established except for the effect of perceived risk on actual disclosure. However, this is acceptable given that recent research has demonstrated that the effect of perceived risk is minimized when strong privacy assurances are given [30].

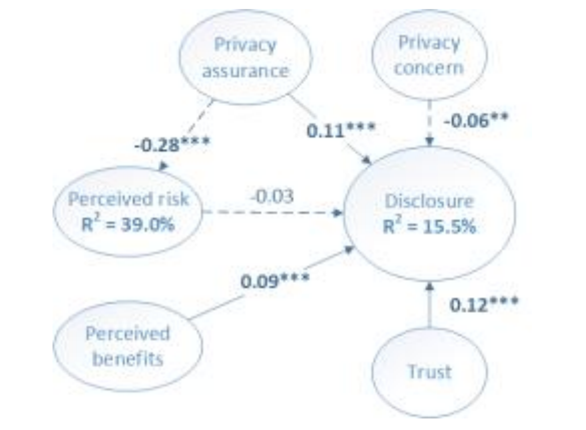

Figure 1. Variance Model of Privacy Calculus

Table 2. Summary of Design Factor Effects

	DIS	ATT	PB	PR	PA	TRU
Gender	0.00	-0.02	-0.05*	0.05*	-0.05*	-0.06*
Color	-0.01	0.03*	0.01	-0.02	0.02	0.02
Animation	0.01	0.00	-0.00	0.02	0.01	0.01
Music	0.01	0.03	0.03	-0.03	0.04†	0.02
Control variable "Attention paid to video"						
Attention	-0.10***	n/a	0.04*	0.04*	-0.08***	-0.08***
Content control variables						
What	-0.03*	NA		0.12***	-0.06**	-0.07***
How	0.06*			0.01	-0.01	-0.02
Who	-0.07*			-0.09**	0.05*	0.10***
ContentFit	0.05*			-0.07***	0.06**	0.07***
ShareRisk	0.12***			-0.05*	0.05*	0.14***

Notes: DIS = actual disclosure, ATT = attention paid to the video, PB = perceived benefits, PR = perceived risk, PA = privacy assurance, TRU = trust in the provider, What = whether the video included "what" data would be collected (0=no, 1=yes), How = whether the video included "how" the data would be used (0=no, 1=yes), Who = whether the video included "who" the data would be shared with (0=no, 1=yes), ContentFit = whether the data collected "fit" the requirements of the app (0=no, 1=yes), ShareRisk = whether the data would be shared with partners (0=no, 1=yes).

To be clear, the purpose of this paper is not to test privacy calculus theory. Rather, we use this model to fully validate our measures in a nomological model as suggested by experts on scale development [38]. Based on the results in Figure 1 confirming privacy calculus theory [15, 34], we conclude that the latent constructs were measured accurately. Therefore, we proceed by calculating participants' factor scores for each latent construct in Figure 1. We also use the actual disclosure variable in its original form (percent of information disclosed) and average the two "attention" items to which we referred earlier.

The purpose of this experiment is to validate the design factors of privacy policy videos to determine their effect on each variable in the model depicted in Figure 1. Accordingly, Table 2 summarizes the results of another PLS model that is based on Figure 1 but also includes the effects of each video design factor as well as the control factors for video content, content fit, and sharing risk (drawn from prior research) [30]. The scores in Table 2 are the coefficients of the PLS algorithm representing the effects of each variable down the left column on each variable across the top.

For simplicity, Table 2 does not include the relationships already analyzed in Figure 1. As before, we measured significance based on a bootstrapping procedure using 1000 samples.

5. Discussion and Implications

The results of the evaluation were quite interesting and leave room for future research. The most important design factor for privacy policy videos is the gender of the narrator voice. In particular, female narrators lead to greater perceived benefits, lower perceived risk, greater feelings of privacy assurance, and greater trust. According to privacy calculus theory [15, 34], this means that female narrators should also result in greater consumer information disclosure.

In addition, vibrant colors lead to greater focus and attention paid to the privacy policy. This effect could be a double-edged sword. On one hand, regulators and consumers would be happy about being able to pay more attention. On the other hand, both prior research [55] and our current results (ß = -0.10, p < 0.001) indicate that as consumers pay attention to privacy policies, they are less likely to disclose information, which is bad for providers. Although using vibrant colors causes consumers to pay closer attention and, thus, possibly be less likely to disclose information, there is also evidence that once consumers begin paying attention to privacy policies, their risk concerns can be reduced by privacy policies' inclusion of appropriate content [30]. Indeed, our control variables indicate that telling consumers *how* their data will be used (ß = 0.06*), having appropriate "fit" between the data collected and the data required for app functionality (ß = 0.05*), and reducing the number of entities with whom consumers' information is shared (ß = 0.12***) can all further increase consumer disclosure once a privacy policy is viewed.

Lastly, using a lighter musical tone did have a marginally significant effect on consumer's feelings of privacy assurance (ß = 0.04, $p < 0.10$).

It is important to place these findings in perspective. Although the design elements of video privacy policies were the focus of this study, and clearly play an important role in risk perceptions and disclosure behavior, the content of a privacy policy is certainly the most important element of a privacy policy [30]. Telling consumers only *what* information will be collected will increase perceived risk and reduce trust, privacy assurance, and disclosure, but disclosure can be somewhat increased by telling consumers *how* their information will be used. More importantly, having an appropriate fit between the data stated to be collected and the apparent requirements of the app can offset the negative effects of telling consumers what data will be collected. Finally, telling consumers *who* their data will be shared with has mixed and surprising—yet very significant—effects. In particular, telling consumers who their data will be shared with appears to reduce disclosure overall, but disclosure is increased if consumers are told that their data will be shared with partners rather than with "nobody."

Some providers may perceive our findings as an opportunity to optimize privacy policy videos to simply maximize consumer information disclosure. That is not our intention. Rather, by identifying the effects of privacy policy video design elements—and, specifically, by designing a video in which these design elements are optimized to minimize perceived risk, maximize trust, and maximize information disclosure, we hope to inform consumers, providers, and regulators. Armed with our findings, regulators can better establish relevant standards for privacy policies and thus protect consumers without over-limiting providers; consumers can be conscious of factors that may influence their perceptions of privacy policy statements delivered through video; and providers can minimize consumers' perceived risk and maximize consumer attention to trust-engendering information.

5.2. Limitations and Future Research

Although we take a design science approach to this topic, it is difficult to assert that the privacy policy videos become part of any designed system. However, an effective privacy policy that elicits compliance from its constituents is a powerful part of systems development and design, assuming that a "security-is-baked-in" approach is desired. Research into IT/IS phenomena will continue to operate on an imperative that IT practice should be improved as we improve our understanding of phenomena from a scientific approach [39]. Thus, while our use of in-situ surveying and hypothesis testing may appear to not be consistent with some canonical assumptions on design science work, our aim is consistent with Hevner's three cycle model [23] of design science research; we strive, in our investigation of effective privacy policy design, to maintain a realistic environment in which to test our design while also providing a "laboratory"-like level of control.

A possibility for future research would be to use embedding in the app ecosystem (the device, distribution channels, and any attendant supporting systems) to measure and analyze app behavior as it pertains to privacy policy understanding. Among the questions to pose would be the degree to which trust changes over time as information asymmetry changes during the producer-consumer relationship. In many circumstances, privacy policies and other terms-of-use agreements change over time. Is the initial trust barrier the only that must be overcome? Would the design of mediated content change depending on the progress of the relationship? What is the right portfolio of information and communication approaches as the relationship progresses (although [30] have made significant progress toward this end)? Further, the diffusion of the artifact itself, the ebb and flow of its community of use, would change.

Another avenue for exploration would then be the degree to which information asymmetry can be reduced from a co-creative position [56]. The co-creation of value, achieved in part via reduction in information asymmetry, could be thought of as bi-directional. If an app like Sharing Tree was developed in a co-creative mode, then the proximity of its user community, accustomed to regular and equitable exchange with producers, would likely have a positive impact on privacy calculus factors such as trust, risk/benefit, and general privacy concerns. This is not a panacea approach, however, as the producer must be prepared for the imperatives that will arise from this arrangement.

A further avenue for research would be to more closely study the flux of information asymmetry itself. This would continue to focus on various mediated content in assistance to the central endeavor of trust-building and the development of shared context between the producer and consumer. The initial hurdle of trust and disclosure, as outlined in this paper, undoubtedly remains important. However, as an instrument of signification, the mediated content is one element in a system of framed actions (actions with the intent of establishing a frame of meaning and understanding) that may be better understood from Activity Theory [16, 47]. Also used in some Human-Computer Interaction studies, Activity Theory would provide some agency to the mediated content to understand how, as a medium, the videos are being used as an intercessor between the producer and consumer—reconciling their worldviews. In this sense, the mediated content of video is creating a learning environment that would reduce information asymmetry. While the components of "first impressions" discussed here are imperative to facilitating a longer-term and potentially co-creative relationship, these are important next-step considerations once the relationship progresses past the who, what, and why results of our study. Entering the fray of high-affect mediated content comes with some responsibility to accept the closeness of the relationship it is likely to foster.

It may be argued that the effect size of our dependent variable, information disclosure, is too low ($R^2 = 15.5\%$). However, given that we measured actual behavior rather than perceptions or intentions, this effect size actually compares quite favorably to that achieved in prior research on consumer information disclosure [31]. Furthermore, as the dependent variable was measured separately (and differently) than the independent variables, there is no possibility for common methods bias, which typically inflates effect sizes in survey-only methodologies [54].

6. Conclusion

In summary, our results indicate that the "best" design for privacy policy videos is one that uses a female narrator to reduce perceived risk and increase trust and assurance, a vibrant color scheme to help consumers pay closer attention, and a light musical tone to increase privacy assurance. Furthermore, it is important that privacy policies include information about *what* data will be collected that "fits" the actual data requirements that are apparent to consumers. However, telling consumers *who* their data will be shared with should be done with care; it has a strong effect on consumer information disclosure, but consumers do not appear to trust providers when they are told that their data will be shared with "nobody."

7. References

[1] A. Acquisti, "Nudging privacy: The behavioral economics of personal information", IEEE Security & Privacy, 7 (2009).

[2] A. Acquisti, L. Brandimarte and G. Loewenstein, "Privacy and human behavior in the age of information", Science, 347 (2015), pp. 509-514.

[3] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor and Y. Agarwal, "Your location has been shared 5,398 times!: A field study on mobile app privacy nudging", *33rd Annual ACM Conference on Human Factors in Computing Systems*.

[4] E. B. Andrade, V. Kaltcheva and B. Weitz, "Self-disclosure on the web: The impact of privacy policy, reward, and company reputation", NA-Advances in Consumer Research Volume 29 (2002).

[5] Apple, "Apple App Store requirements on privacy and data collection and storage", https://developer.apple.com/app-store/review/guidelines/ - legal, Accessed on May 30, 2017.

[6] J. Babb, K. Dana, M. Keith and M. Jafar, "Evolving Mobile Architectures: A Case Study in the Development of a Location Privacy Application", *Conference on Information Systems Applied Research ISSN, New Orleans, LA*.

[7] F. Bélanger and R. E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems", MIS Quarterly, 35 (2011), pp. 1017-1041.

[8] P. E. Bestelmeyer, P. Maurage, J. Rouger, M. Latinus and P. Belin, "Adaptation to vocal expressions reveals multistep perception of auditory emotion", Journal of Neuroscience, 34 (2014), pp. 8098-8105.

[9] C. Breuer and C. Rumpf, "The Impact of Color and Animation on Sports Viewers' Attention to Televised Sponsorship Signage", Journal of Sport Management, 29 (2015), pp. 170-183.

[10] N. R. Buchan, R. T. Croson and S. Solnick, "Trust and gender: An examination of behavior and beliefs in the Investment Game", Journal of Economic Behavior & Organization, 68 (2008), pp. 466-476.

[11] M. Buhrmester, T. Kwang and S. D. Gosling, "Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data?", Perspectives on psychological science, 6 (2011), pp. 3-5.

[12] E. Commission, "Article 29: Data protection working party: Opinion on apps on smart devices", http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf, February 27, 2013, Accessed on May 30, 2017.

[13] E. Commission, "Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union", http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, June 2011, Accessed on June 9th, 2016.

[14] F. T. Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers", https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, March 2012, Accessed on May 26, 2017.

[15] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions", Information Systems Research, 17 (2006), pp. 61-80.

[16] Y. Engeström, R. Miettinen and R.-L. Punamäki, *Perspectives on activity theory,* Cambridge University Press, 1999.

[17] C. Flavián and M. Guinalíu, "Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site", Industrial Management & Data Systems, 106 (2006), pp. 601-620.

[18] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error", Journal of Marketing Research, 18 (1981), pp. 39-50.

[19] S. E. Gindin, "Nobody reads your privacy policy or online contract: Lessons learned and questions raised by the FTC's action against Sears", Nw. J. Tech. & Intell. Prop., 8 (2009), pp. 1.

[20] G. J. Gorn, A. Chattopadhyay, T. Yi and D. W. Dahl, "Effects of color as an executional cue in advertising: They're in the shade", Management science, 43 (1997), pp. 1387-1400.

[21] M. A. Graber, D. M. D'alessandro and J. Johnson-West, "Reading level of privacy policies on Internet health Web sites.(Brief Report)", Journal of Family Practice, 51 (2002), pp. 642-646.

[22] S. Gregor and D. Jones, "The anatomy of a design theory", Journal of the Association for Information Systems, 8 (2007), pp. 312-335.

[23] A. R. Hevner, "A three cycle view of design science research", Scandinavian journal of information systems, 19 (2007), pp. 4.

[24] A. R. Hevner, S. T. March, J. Park and S. Ram, "Design Science in Information Systems Research", MIS Quarterly, 28 (2004), pp. 75-105.

[25] K. Hung, "Framing meaning perceptions with music: The case of teaser ads", Journal of advertising, 30 (2001), pp. 39-49.

[26] J. Jaiswal, "Location-Aware Mobile Applications: Privacy Concerns & Best Practices", Accessed on April 5th, 2012.

[27] M. Keith, J. Babb, P. B. Lowry, C. Furner and A. Abdullat, "Limited Information and Quick Decisions: Consumer Privacy Calculus for Mobile Applications", AIS Transactions on Human-Computer Interaction, 8 (2016), pp. 88-130.

[28] M. J. Keith, J. Babb and P. B. Lowry, "A Longitudinal Study of Information Privacy on Mobile Devices", *47th Hawaiian International Conference on Systems Sciences (HICSS 2014), Big Island, Hawaii, January*.

[29] M. J. Keith, J. S. Babb, P. B. Lowry, C. P. Furner and A. Abdullat, "The role of mobile-computing self-efficacy in consumer information disclosure", Information Systems Journal, 25 (2015), pp. 637-667.

[30] M. J. Keith, K. S. Reeves, J. T. Fredericksen and J. S. Babb, "Resolving the Privacy Policy Paradox with Content-Optimized Videos", *Dewald Roode Workshop on Information Privacy and Security, IFIP WG 8.11/11.13, St. Pete Beach, FL,* October 6-7, 2017.

[31] M. J. Keith, S. C. Thompson, J. Hale, P. Benjamin Lowry and C. Greer, "Information Disclosure on Mobile Devices: Re-examining Privacy Calculus with Actual User Behavior", International Journal of Human-Computer Studies, 71 (2013), pp. 1163–1173.

[32] M. J. Keith, S. C. Thompson, J. Hale and C. Greer, "Examining the Rationality of Information Disclosure through Mobile Devices", *International Conference on Information Systems (ICIS '12), Orlando, FL,* December 16-19, 2012.

[33] G. Lakoff and M. Johnson, *Metaphors we live by*, University of Chicago press, 2008.

[34] R. S. Laufer and M. Wolfe, "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory", Journal of Social Issues, 33 (1977), pp. 22-42.

[35] H. A. Lee, N. Au and R. Law, "Presentation formats of policy statements on hotel websites and privacy concerns: a multimedia learning theory perspective", Journal of Hospitality & Tourism Research, 37 (2013), pp. 470-489.

[36] R. Lohtia, N. Donthu and E. K. Hershberger, "The impact of content and design elements on banner advertising click-through rates", Journal of advertising Research, 43 (2003), pp. 410-418.

[37] P. B. Lowry, G. Moody, A. Vance, M. Jensen, J. Jenkins and T. Wells, "Using an Elaboration Likelihood Approach to Better Understand the Persuasiveness of Website Privacy Assurance Cues for Online Consumers", Journal of the American Society for Information Science and Technology, 63 (2012), pp. 755-776.

[38] S. B. MacKenzie, P. M. Podsakoff and N. P. Podsakoff, "Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques", MIS quarterly, 35 (2011), pp. 293-334.

[39] S. T. March and G. T. Smith, "Design and Natural Science Research on Information Technology", Decision Support Systems, 15 (1995), pp. 251-266.

[40] R. E. Mayer, "Cognitive theory and the design of multimedia instruction: an example of the two-way street between cognition and instruction", New directions for teaching and learning, 2002 (2002), pp. 55-71.

[41] R. E. Mayer, "Multimedia learning: Are we asking the right questions?", Educational psychologist, 32 (1997), pp. 1-19.

[42] R. E. Mayer and R. Moreno, "Nine ways to reduce cognitive load in multimedia learning", Educational psychologist, 38 (2003), pp. 43-52.

[43] A. M. McDonald and L. F. Cranor, "The cost of reading privacy policies", ISJLP, 4 (2008), pp. 543.

[44] S. Mlot, "EU: This Is How We Would Improve Google's Privacy Policy", http://www.pcmag.com/article2/0,2817,2469314,00.asp, September 26, 2014, Accessed on May 26, 2017.

[45] M. M. Mormann, V. Navalpakkam, C. Koch and A. Rangel, "Relative visual saliency differences induce sizable bias in consumer choice", (2012).

[46] S. Musil, "California gives teens an 'eraser button' to hide online skeletons", http://news.cnet.com/8301-1009_3-57604301-83, September 23rd, 2013, Accessed on October 1st, 2013.

[47] B. A. Nardi, *Context and consciousness: activity theory and human-computer interaction*, Mit Press, 1996.

[48] P. A. Norberg, D. R. Horne and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors", The Journal of Consumer Affairs, 41 (2007), pp. 100-126.

[49] R. M. O'Brien, "A caution regarding rules of thumb for variance inflation factors", Quality & Quantity, 41 (2007), pp. 673-690.

[50] Y. Pan and G. M. Zinkhan, "Exploring the impact of online privacy disclosures on consumer trust", Journal of Retailing, 82 (2006), pp. 331-338.

[51] E. Peer, J. Vosgerau and A. Acquisti, "Reputation as a sufficient condition for data quality on Amazon Mechanical Turk", Behavior Research Methods, 46 (2014), pp. 1023-1031.

[52] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chatterjee, "A design science research methodology for Information Systems Research", Journal of Management Information Systems, 24 (2007), pp. 45-77.

[53] B. J. Phillips and E. F. McQuarrie, "Beyond visual metaphor: A new typology of visual rhetoric in advertising", Marketing theory, 4 (2004), pp. 113-136.

[54] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee and N. P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies", Journal of Applied Psychology, 88 (2003), pp. 879-903.

[55] I. Pollach, "What's wrong with online privacy policies?", Communications of the ACM, 50 (2007), pp. 103-108.

[56] C. K. Prahalad and V. Ramaswamy, "Co-creation experiences: The next practice in value creation", Journal of interactive marketing, 18 (2004), pp. 5-14.

[57] C. M. Ringle, S. Wende and J.-M. Becer, "SmartPLS 3", Boenningstedt: SmartPLS GmbH, http://www.smartpls.com/ (2015).

[58] P. Samuelson, *Information Law and Policy Video Lectures*, UC California, Berkeley, Berkeley, CA, USA, 2008.

[59] J. R. A. Santos, "Cronbach's alpha: A tool for assessing the reliability of scales", Journal of extension, 37 (1999), pp. 1-5.

[60] L. M. Scott, "Understanding jingles and needledrop: A rhetorical approach to music in advertising", Journal of Consumer Research, 17 (1990), pp. 223-236.

[61] H. J. Smith, T. Dinev and H. Xu, "Information privacy research: An interdisciplinary review", MIS Quarterly, 35 (2011), pp. 989-1015.

[62] J. Y. Tsai, S. Egelman, L. Cranor and A. Acquisti, "The effect of online privacy information on purchasing behavior: An experimental study", Information Systems Research, 22 (2011), pp. 254-268.

[63] D. Wilson and J. S. Valacich, "Unpacking the privacy paradox: Irrational decision-making within the privacy calculus", (2012).

[64] L. D. Wolin, "Gender issues in advertising", Journal of advertising research, 43 (2003), pp. 111-130.

[65] T. L. Wright and E. G. Sharp, "Content and grammatical sex bias on the Interpersonal Trust Scale and differential trust toward women and men", Journal of Consulting and Clinical Psychology, 47 (1979), pp. 72.

[66] K.-W. Wu, S. Y. Huang, D. C. Yen and I. Popova, "The effect of online privacy policy on consumer privacy concern and trust", Computers in human behavior, 28 (2012), pp. 889-897.

[67] H. Xu, X. Luo, J. M. Carroll and M. B. Rosson, "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing", Decision Support Systems, 51 (2011), pp. 42-52.

[68] H. Xu, H. H. Teo, B. C. Y. Tan and R. Agarwal, "The role of push-pull technology in privacy calculus: The case of location-based services", Journal of Management Information Systems, 26 (2010), pp. 135-174.