Rational Ignorance and Privacy Risk Information Seeking

Early-stage paper

Craig Van Slyke
Louisiana Tech University
vanslyke@latech.edu

Grant Clary
Tennessee Tech University
gclary@tntech.edu

Mihir Parikh
New York University
mihir@nyu.edu

Damien Joseph
Nanyang Technological University
adjoseph@ntu.edu.sg

ABSTRACT

As life becomes increasingly digital, protecting one's privacy grows in importance. Understanding factors that influence privacy-related behaviors is a topic of continuing interest to privacy researchers. In this paper, we report on an early-stage study that investigates the effects of rational ignorance on privacy risk information seeking. Rational ignorance concerns the effects of perceived information acquisition costs and benefits on information-seeking activities. When an individual believes that the costs of acquiring information exceed the anticipated benefits of that information, the individual will not seek the information. To investigate the effects of rational ignorance calculus on a privacy risk information-seeking behavior (reading an app's privacy policy), we conducted eight interviews with attendees of a conference that required participants to use a COVID-19 vaccination status app. The interviews revealed that rational ignorance calculus does impact whether the interviewees read the app's privacy policy, but this effect was moderated by the interviewee's privacy identity. Individuals who viewed themselves as privacy experts were less affected by rational ignorance calculations; they read the app's privacy policy regardless of the anticipated costs and benefits. Others did not read the privacy policy because they did not view

it as beneficial to their decision to use the app. In addition, trust in the association sponsoring the conference and in the app's developer affected rational ignorance calculus.

Keywords

Rational ignorance, rationality, rational decision-making, irrationality, privacy, privacy calculus, privacy paradox.

INTRODUCTION

Factors affecting privacy decisions have long been an area of interest to privacy researchers. This has been reflected primarily in research into two privacy decisions: information-disclosure decisions and privacy-protection decisions. Rational choice theory serves as the foundation for many studies of privacy-related behaviors. Essentially, rational choice theory proposes that when individuals are faced with a choice among alternatives, they will choose the alternative that maximizes the ratio of anticipated benefits to costs (Hernstein, 1990). Privacy researchers have used rational choice theory to examine disclosure decisions, as is the case with privacy calculus. These decisions require information about risks in order to estimate potential costs.

Disclosure of private information involves risk, but the risks are often not readily apparent. So, when individuals encounter a situation in which they believe that their privacy may be at risk, they seek information to reduce the uncertainty associated with the risk. This information may include privacy risk awareness, privacy knowledge, and technology knowledge. This information, when combined with other factors, helps determine the individual's privacy behavior (Crossler & Belanger, 2019). Privacy risk awareness, which concerns the extent to which the individual is aware of the privacy risks associated with a specific context (the use of an app in our case), is of primary interest in our study.

Generally speaking, the more information one has about the benefits and risks associated with a decision, the lower the level of uncertainty with respect to those benefits and risks. Put differently, people use information to reduce uncertainty. Acquiring more information about a risk allows for a more normatively rational decision to be made. However, information acquisition and use are not without cost. So, when making decisions, individuals need to assess the estimated value of the information relative to the estimated costs of acquiring and using the information. If the costs associated with acquiring the information are higher than the benefit of having that information, it would be more rational to stay uninformed. This decision is the basis of the rational ignorance principle.

The relevance of rational ignorance to information privacy has been mentioned (e.g., Acquisti et al., 2007; Barth & de Jong, 2017; Tasi et al., 2020; Van Slyke et al., 2021), but to our knowledge, the rational ignorance principle has not been empirically tested in the context of information privacy. This early-stage work represents an initial attempt to validate the applicability of rational ignorance to privacy-oriented decision-making. Our work investigates the following research question:

Do the perceived costs and benefits of seeking information about privacy risks affect privacy risk information-seeking behavior?

Specifically, we report on the preliminary stages of a multi-method investigation of the application of rational ignorance to the decision to read a mobile app's privacy policy. Preliminary results indicate that rational ignorance calculus (anticipated costs and benefits of seeking, acquiring, and using privacy information) affects decisions to read an app's privacy policy, but those effects are moderated by one's privacy identity. In addition, trust affects rational ignorance calculus. Note

that this is an early-stage report; we anticipate having additional data and analysis to present at the workshop (if accepted).

The remainder of this paper is organized as follows. In the next section, we provide background information on privacy decision-making and risk information seeking. This is followed by a discussion of the rational ignorance principle. Next, we describe the initial stage of our empirical study. We then report preliminary results from this study and provide a preliminary theoretical model. Next, we discuss the implications of our work and describe the later stages of the research project. Finally, we offer some concluding remarks.

BACKGROUND

Privacy decision-making and risk

According to the privacy calculus perspective, people make information disclosure decisions based on their assessment of the relative benefits and risks of the disclosure (Culnan and Armstrong, 1999). But it is unlikely that information will be complete, particularly about risks (Acquisti & Grossklags, 2004). Privacy policies are one source of risk information (as discussed further below). So, using privacy calculus as a lens, we posit that an individual facing a privacy-related decision will first face a decision regarding whether to seek additional information about privacy risks (which we refer to as risk information). The rational ignorance principle indicates that the decision-maker will seek additional information only up to the point at which the perceived utility of the information exceeds the anticipated costs of acquiring that information.

To further understand the role of risk information in privacy behaviors, we can turn to protection motivation theory (PMT) (Rogers, 1975), which has been applied to privacy (Floyd et al., 2000). At a high level, PMT indicates that two appraisals, a threat appraisal, and a coping appraisal,

determine if one engages in protective behaviors. Both of these appraisals require information, and both are characterized by some extent of uncertainty. The threat appraisal considers the perceived severity of the privacy threat and the perceived extent to which one is vulnerable to the privacy threat. The coping appraisal involves assessing one's ability to enact protective measures and the effectiveness of those measures. All of these appraisals are characterized by uncertainty; one cannot know the full extent of the threat. One antidote to uncertainty is information; people may seek information that can reduce the perceived uncertainty of these appraisals, which increases the confidence one has in their perceptions. So, it is clear that information plays a role in privacy decision-making. In many cases, the privacy decision-maker does not possess all relevant information. As a result, it is important to understand how individuals make decisions regarding the acquisition of privacy risk information.

Privacy Policies

Privacy policies are one source of information that is relevant to privacy decision-making (van Oojien et al., 2022). An argument can be made that understanding what information is collected and how that information is used is fundamental to understanding the privacy risks associated with using a website or app. While some of these risks can be mitigated, it is unlikely that a user can protect against all privacy risks brought on by an app. In fact, some apps require identifying information in order to function. For example, apps directed at identifying an individual require the disclosure of personal information in order to operate. Privacy policies typically include some information related to risk, such as how disclosed data will be used and shared, and may also include information about some protective measures, such as deleting private data.

Privacy policies and regulations focus on providing notice, awareness, and consent related to data usage. Privacy policies improve transparency of how the company is adhering to governmental

regulations and industry standards. Even more, privacy policies are usually accessible;[1] most companies have their privacy policy publicly available at the bottom of their web pages (Jensen & Potts, 2004), for example. Having transparent privacy policies is intended to improve one's trust in an organization (Ermakova et al., 2014; Wu et al., 2012).

Unfortunately, privacy policies are not read by the typical consumer (Obar and Oeldorf-Hirsch, 2018). A 2008 study estimated that Internet users in the United States would spend about 244 hours per year to read website privacy policies they encounter (McDonald and Cranor 2008). Privacy policies are often long and opaque (Wilson et al., 2016). Reading and attempting to understand the meaning of a policy requires considerable time and cognitive effort (Proctor et al., 2008; Meier et al., 2020). To complicate things further, privacy policies can change frequently (Wilson et al., 2016), leaving it to the consumer to keep up with the most up-to-date version and changes from previous versions.

Rational ignorance principle

When individuals are deciding whether or not to seek information to use in decision-making, the rational ignorance principle comes into play. Downs (1957) describes the rational ignorance principle thusly, "The information-seeker continues to invest resources in procuring data until the marginal return from information equals its marginal cost. At that point, assuming decreasing marginal returns or increasing marginal costs, or both, he has enough information and makes his decision" (p. 215). In other words, under rational ignorance, a decision-maker will seek information only as long as the perceived marginal benefit from the information exceeds the

[1] We acknowledge that although policies are typically readily available, obfuscating language may make the information less accessible.

perceived marginal acquisition costs. Although Downs developed the concept of rational ignorance in the context of voter information seeking, the principle can be applied to virtually any context that involves rational decision-making.[2]

In terms of privacy risk information, an individual will seek information regarding a privacy risk only up to the point at which the perceived additional benefits of the information exceed the information's value in making the decision regarding whether to seek additional information. Several researchers have noted that rational ignorance may help inform information privacy research (e.g., Acquisti et al., 2007; Barth & de Jong, 2017; Tasi et al., 2020; Van Slyke et al., 2021). However, to our knowledge, there are no published empirical investigations of rational ignorance in the context of information privacy. The most complete conceptual treatment of rational ignorance as it relates to privacy comes from Van Slyke et al. (2021), who compared rational ignorance to several similar concepts, including privacy cynicism (Hoffmann et al., 2016), privacy resignation (Wirth et al., 2018), and privacy fatigue (Choi et al., 2018), concluding that rational ignorance was substantially distinct from these concepts. In addition, rational ignorance differs from information avoidance. Information avoidance involves purposefully ignoring information due to the threat posed by the information. In contrast, rational ignorance posits that individuals fail to seek information not because of the threat it poses, but rather because it is not worth the cost.

As noted earlier, information regarding privacy risks is important to information to the privacy calculus and to making decisions regarding protective behaviors. Therefore, when considering

[2] Note that privacy decisions are not always the result of conscious deliberation.

information disclosure, individuals face a decision regarding whether to seek information that can help them better understand the risks involved with disclosing information. They may also seek information regarding potential ways to protect their privacy, such as data deletion policies and procedures or how to correct information errors. In addition, app privacy policies seem especially subject to rational ignorance effects because 1) privacy policies are focused on providing information, and 2) many mobile apps require agreeing to the privacy policy prior to use. So, often users must decide whether to read the privacy policy when installing an app, making the behavior a choice task. For these reasons, we use the context of disclosing sensitive information via a mobile app to study the effects of rational ignorance. In the following section, we describe the initial stage of the study.

METHOD

In order to understand the role of rational ignorance in privacy risk assessment, we are undertaking a multi-phase, multi-method study. This early-stage paper reports the preliminary results from the first phase, a qualitative study that seeks to determine whether rational ignorance applies to privacy protection and to better understand the nomological network associated with rational ignorance and privacy protection. Once complete, we will use the results of the qualitative phase to test specific causal paths derived from the qualitative results.

The genesis of this study came during an academic conference that required the use of the Clear app to provide proof of one's COVID-19 vaccination status. Informal conversations regarding the Clear app indicated that many attendees did not bother to read the privacy policy because they were already committed to attending the conference. We noticed that these individuals felt that they had to download and use the app, even if the privacy policy was problematic. This is a classic illustration of rational ignorance – these attendees chose to remain ignorant of Clear's privacy

policy (and the risk and protection information it contained) because they felt it made no difference in their use of the app. Because these were informal conversations, they were not documented, and specific information from these conversations is not used in our analysis. However, these interesting enlightenments gave us the motivation to pursue a formal investigation.

After the conference, our research team met and developed an interview protocol. After the protocol was approved by the appropriate research ethics committee, interviews were scheduled with individuals who were known by the research team to have attended the conference. To date, we have interviewed eight users of a mobile app (Clear), the use of which was required for attendance at an academic conference.[3] We believe that this is a useful context in which to study rational ignorance effects. The interviews remained focused on the research question, and as a result, they were relatively short. The mean interview time was approximately eleven minutes. Although the interviews followed the protocol, we did pursue interesting avenues of discussion when deemed appropriate. Interviews were conducted online and recorded. The recordings were then transcribed.

The interviews were coded iteratively. The first round of analysis looked for mentions of factors related to rational ignorance. This initial round surfaced several other interesting factors, including trust in the conference organizers, trust in the app developers, and privacy identity. So, another round of analysis was conducted to look for comments associated with these factors.

[3] The Clear app was required of domestic attendees in order to document COVID-19 vaccine status. Conference management informed attendees of this requirement shortly before the conference. Note that one interviewee did not use the Clear app but did use the mobile app the conference organizers used for the conference program.

This is a convenience sample, but we believe this is acceptable at this stage of the research. We are not claiming statistical generalizability; we are only seeking to demonstrate the existence of the rational ignorance principle in the context of privacy risk information-seeking behaviors and to gain an initial understanding of relevant factors. Note that we plan to conduct and analyze additional interviews prior to the workshop. Also note that the analysis is still preliminary at this point. However, as discussed in the next section, we are encouraged by the results so far.

RESULTS

Our overarching research question concerns whether the perceived costs and benefits of seeking privacy-related information affect privacy risk information seeking. In other words, does the rational ignorance principle apply to privacy risk information seeking? Our interviews to date clearly illustrate that the answer to this question is yes, but with mitigating factors. In this section, we discuss our findings to date, starting with the effect of rational ignorance, then proceed to factors that seem to affect or moderate the effect of rational ignorance calculus.

Rational Ignorance

The clearest indication of the rational ignorance policy at work came from an interviewee who indicated that they did not read the Clear app's privacy policy. When the interviewer asked why not, the interviewee responded, "*Because it didn't matter."* This led the interviewer to ask for further explanation. The interviewee explained that they had already booked and paid for the conference, and they were obligated to attend. Therefore, they felt that there was no point in reviewing the privacy policy because they 1) felt obligated to attend the conference, and 2) the app was required for conference attendance.

Another interviewee expressed similar sentiments. When asked why they hadn't carefully read the privacy policy, the interviewee responded, *"I didn't think it really mattered; I had to use it to attend the conference."* Another interviewee started reading the privacy policy but stopped when they *"had this sudden revelation that the conference required you to provide proof of vaccination, and the only way you could really provide proof of vaccination was to use the app."* So, they stopped reading the privacy policy.

Cost/benefit reasoning was directly expressed by an interviewee that stated, *"Because honestly, if you want to go to the conference, and I needed to go, so I'm like 'I just don't have time for this.' Because it's cost/benefit, right? If I spend any time [reading the privacy policy], … I'm going to have to go anyway. So why spend a bunch of time …"*

Our analysis also revealed that trust played a role in rational ignorance calculus. We discuss this below.

Trust

Two interviewees indicated that they decided not to read the app's privacy policy because they depended on the organization sponsoring the conference (Association for Information Systems (AIS)). One stated that they did not read the privacy policy *"… because I'm sure AIS did their due diligence in protecting us from anything that is suspicious. I was counting on the AIS."* Another said they *"… trust AIS to have my best interest [in mind]."*

These comments were interesting in light of the original work on rational ignorance. Downs (1957) wrote at length about the role of political parties, media outlets, and other organizations in providing information regarding political candidates. Such organizations are effectively information intermediaries between the individual and the information sources. The organizations

sift through relevant information and condense it, sometimes to something as simple as an endorsement, reducing the information acquisition costs to the decision-maker.

However, these information intermediaries are not effective unless they are deemed as trustworthy by the decision-maker. This also seems to be the case with privacy information acquisition. The earlier statement about AIS doing their due diligence is a clear indication that the interviewee trusted AIS to not only be competent in assessing the privacy risks and protections associated with the Clear app, but also to be benevolent in keeping the users' privacy in mind. Another interviewee brought up trust in AIS more directly, *"... maybe because it's an organization that involves information systems scholars, and so I had some type of trust that ... the information wasn't going to be used for a malicious purpose. I trusted the organization that was rolling out the app. ... I trusted AIS."*

Trust in the app's developers was also a factor for some interviewees. One stated, *"... when I realized, 'Oh, it's the same Clear system at major airports,' that gave me a bit more trust ...".* Another noted that their partner had used the same app to attend a different conference. So, they *"felt more comfortable that it wasn't just some app that was developed by a student. It felt legitimate to me."*

Privacy Identity – Moderating Factor

One interesting insight from our interviews is that the rational ignorance calculus is not absolute. People will act in ways that are counter to the perceived cost and benefits of privacy information acquisition. In other words, they will seek information for reasons beyond the information's perceived value in deciding whether or not to use the app and disclose information. We saw this in three of our participants who read the Clear app's privacy policy despite knowing that they were

going to download and use the app regardless of the contents of the policy. In all three cases, when asked why they read the privacy policy, they referred not to the information's value in deciding whether to use the Clear app, but to other factors. One replied bluntly to the question of why they read the policy, *"[Because it's] my job as a privacy researcher."* Another made a similar statement, *"Because … I'm someone that does research in the area of privacy and security. I just found it interesting."*

Another participant provided a different reason for reading the privacy policy, indicating that they always tried to read the privacy policy. Through other aspects of the interview, we inferred that this individual viewed themself as someone who generally reads privacy policies due to their overall concerns about privacy.

None of these responses mentioned the information's value in determining their use of the Clear app. They decided to read the privacy policy for other reasons. Although this inference is preliminary, we concluded that there was some aspect of the interviewees' personal identities that led them to disregard the rational ignorance calculus and read the privacy policy even though the information in the policy was not used in the decision to use the Clear app. We label this belief one's privacy identity, which we define as the extent to which a person views understanding 1) the benefits and risks of information disclosure and 2) means of protecting oneself from those risks as being integral to their sense of self. Note that this definition is preliminary and is adapted from Carter et al.'s (2020) definition of information technology identity.

Downs (1957) noted a similar situation among voters. He stated that rational voters' actions might be motivated by a sense of duty to democracy rather than their own short-term gains and losses. This parallels to what we found. For the three individuals mentioned above, their self-identities

related to privacy motivated them to read the app's privacy policy regardless of the utility of the information contained therein (with respect to their decision to use the Clear app).

To summarize, we found that rational ignorance calculus was a factor in determining whether participants read the Clear app's privacy policy. However, the effects of the privacy calculus are not absolute. For three of our participants, their personal identities related to privacy effectively negated the rational ignorance calculus, and they read the privacy policy. These effects are shown in Figure 1 below. Please note that at this early stage of our research project, we acknowledge that these results are preliminary.

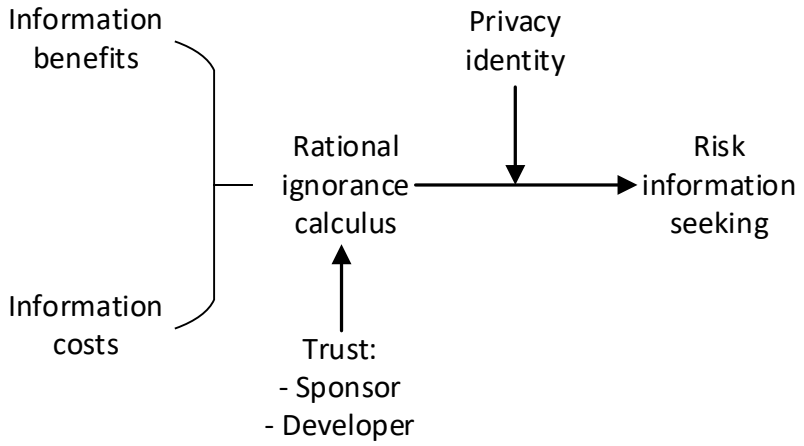

Figure 1 – Preliminary Model

DISCUSSION

Although preliminary, our analysis reveals several interesting results. First, the rational ignorance principle, and rational ignorance calculus, can be applied to understanding information-seeking behaviors in the context of information privacy. This provides a preliminary proof of concept for the application of rational ignorance to information privacy.

Second, although rational ignorance calculus did influence information seeking for some of our participants, this effect was not universal. According to our data, the effect of rational ignorance calculus on information-seeking behavior was moderated by privacy identity. Individuals who exhibited privacy identity read the Clear app's privacy policy even though they indicated that they were going to download and use the app regardless of the privacy policy due to their conference obligations. In other words, they decided to read the privacy policies due to their self-identity as privacy researchers and/or advocates. They acknowledged their reasons for seeking the information from the privacy policy resulted from their identity, not from the value of the information in making the decision to use the Clear app.

This concept of privacy identity differs from Westin's (1991) typology of the privacy fundamentalists, the pragmatic, and the unconcerned. This typology relates to concerns about information disclosures and regulations and was classified according to their privacy concerns and views of the adequacy of privacy regulations (Kumaraguru & Cranor, 2005). It is possible for an individual to be a privacy fundamentalist but not view privacy awareness and knowledge as part of their self-identity. So, we contend that privacy identity is materially distinct from Westin's typology.

In addition, we do not consider the decision to read the privacy policy by privacy identifying individuals as irrational, despite what rational ignorance calculus might predict. Maintaining one's self-identity is important for setting standards of how people behave (Carter et al., 2020). So, even though the value of the privacy policy information was not useful in disclosure decisions, it was important in maintaining and reinforcing self-identity. As Downs' (1957) noted, there are non-utility reasons for engaging in information search; our results reinforce this thinking.

Finally, our findings support the importance of trust in determining the balance of information benefits and costs. The importance of trust in determining disclosure behaviors has a long history. Many early e-commerce studies considered the role of trust and trustworthiness in determining whether to engage online with a merchant (e.g., Ang et al., 2001; Johnston & Warkentin, 2004; Van Slyke et al., 2006). In addition, the effects of privacy policies on trust in an organization has also been studied (e.g., Wu et al., 2012; Esmaeilzadeh, 2020). We take a different view here. In our model, trust affects rational ignorance calculus by reducing the perceived benefits of information seeking. When our participants trusted AIS, the decision-making value of seeking additional information regarding privacy risks is reduced. The participants that trusted AIS would expect to gain less from reading the privacy policy because they expected AIS to have already vetted Clear's privacy policies and practices.

AIS could have played a different important role by making the Clear app's privacy policy more accessible and understandable in order to reduce the costs of obtaining the information contained in the policy. For example, AIS might have included an overview of the most important parts of the privacy policy in the email informing attendees of the required use of the app. This information intermediary role is important; there are many instances of advocacy and trusted third parties taking steps to reduce information search costs. For example, political parties obtain information about candidates and make it more readily available to voters, reducing their search costs (Downs, 1957). Similarly, third-party privacy seals served a similar purpose in e-commerce (Belanger et al., 2002).

Making the information contained in privacy policies more accessible is important. Although privacy policies are often easy to locate (Jensen & Potts, 2004), they are often opaque, sometimes intentionally so. This increases information search costs, which may lead to people concluding

that their effort of understanding the contents of privacy policies is not offset by the benefits of the information. Trusted third parties can help shift this calculus by reducing information search costs.

For some participants, trust in the Clear app's developer was also important. They had knowledge of Clear in other contexts, and this knowledge transferred to the current situation. These individuals have favorable impressions of Clear's privacy practices, so they found it less useful to seek additional information. However, had their view of Clear's privacy practices been negative, this may have increased the value of additional information seeking, although this is supposition at this point.

Contributions

Our work makes four main contributions. First, we provide an empirical examination of the applicability of the rational ignorance principle to information privacy. Essentially, our results provide a sort of "proof-of-concept" that rational ignorance can be applied to information privacy information seeking. Although our work is only an initial step, we believe that rational ignorance provides a novel lens through which to examine information-seeking behaviors related to information privacy decisions.

Second, our model gives an initial view of how rational ignorance affects privacy information-seeking behaviors. The model needs to be further developed and validated, but the model inferred from our data provides a useful foundation for further research into rational ignorance calculus and information privacy decisions and behaviors, especially since we studied actual information-seeking behaviors rather than intentions.

Third, we identify privacy identity as an important construct and demonstrate its moderating effect. The extent to which understanding privacy risks and benefits is a part of one's self-identity is an

interesting avenue for further exploration. Recent work on information technology identity (e.g., Carter & Grover, 2015; Carter et al., 2020) indicates that the extent to which a person's sense of self is tied to their use of information technology affects their behavioral choices. We demonstrate that one's privacy identity similarly affects privacy information-seeking behaviors.

Finally, the importance of trust in privacy decision-making is well established. Our work uncovers an under-studied role of trust – its influence on the utility of privacy information. We demonstrate that trust in two third parties, a professional association, and an app developer, affects rational ignorance calculus, primarily through reducing the expected value of information, which subsequently affects privacy information seeking. This view strengthens the idea that trust is not monolithic with respect to information privacy. There are many parties involved in information privacy, and the trustworthiness varies among these. A fuller understanding of information privacy decisions requires considering the extent to which users are willing to trust the various parties involved and the impacts of these trust assessments.

Limitations

Our work is subject to several limitations. Our sample size is small and is comprised of members of an idiosyncratic population. So, it is important to expand investigations of rational ignorance to broader populations. A similar statement can be made about context. We studied a particular app, which was mandated for attendance at an academic conference; this may exacerbate the effects of rational ignorance calculus. Further research is necessary to determine whether our initial model holds across populations and contexts. Finally, our analysis is preliminary and is subject to researcher bias in the interpretations of our data. We expect to have additional interview data prior to the workshop, which may allow us to strengthen our findings through a more robust analysis of the interview data. We hope to provide the results of this additional analysis at the workshop if our

work is accepted. Once our theoretical model is fully developed, we will collect survey data to test the model, but we do not expect to have these data available prior to the workshop.

CONCLUSIONS

A rational choice is made when one performs a cost-benefit analysis before engaging in a behavior. Therefore, if one were to make a rational choice about disclosing private information online, the rational actor would gather information associated with the costs (i.e., risks) and benefits of the disclosure. However, information seeking comes with a cost. As a result, the individual must decide how much information to seek. The rational ignorance principle states that people will seek information only when the benefits of that information are expected to exceed the costs of acquiring the information.

In this paper, we demonstrate that the rational ignorance principle can be applied to information privacy decisions by analyzing data from interviews of attendees of an academic conference. We develop the first (to our knowledge) empirically derived model of rational ignorance in the context of information privacy decision-making. Even though our model is preliminary, our work, and the model, hold implications for information privacy research.

REFERENCES

Acquisti, A., Gritzalis, S., Lambrinoudakis, C., & di Vimercati, S. (2007). What can behavioral economics teach us about privacy?. In *Digital Privacy* (pp. 385-400). Auerbach Publications.

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. In *Economics of Information Security* (pp. 165-178). Springer, Boston, MA.

Ang, L., Dubelaar, C., & Lee, B. C. (2001). To trust or not to trust? A model of internet trust from the customer's point of view. *BLED 2001 Proceedings*, 43.

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics*, *34*(7), 1038-1058.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3-4), 245-270.

Carter, M., & Grover, V. (2015). Me, my self, and I (T). *MIS Quarterly*, 39(4), 931-958.

Carter, M., Petter, S., Grover, V., & Thatcher, J. B. (2020). Information Technology Identity: A Key Determinant of IT Feature and Exploratory Usage. *MIS Quarterly*, 44(3).

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42-51.

Crossler, R. E., & Bélanger, F. (2019). Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap. *Information Systems Research*, *30*(3), 995-1006.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104-115.

Downs, A. (1957). *An Economic Theory of Democracy*, Boston: Addison-Wesley Publishing Company.

Ermakova, T., Baumann, A., Fabian, B., & Krasnova, H. (2014, August). Privacy policies and users' trust: does readability matter?. *Proceedings of the Twentieth Americas Conference on Information Systems*, Savannah.

Esmaeilzadeh, P. (2020). The impacts of the privacy policy on individual trust in health information exchanges (HIEs). Internet Research, 30(3), 1066-2243.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407-429.

Herrnstein, R. J. (1990). Rational choice theory: Necessary but not sufficient. *American Psychologist*, 45(3), 356.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4).

Jensen, C., & Potts, C. (2004, April). Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (pp. 471-478).

Johnston, A. C., & Warkentin, M. (2004). The online consumer trust construct: a web merchant practitioner perspective. *Proceedings of the 7th Annual Conference of the Southern AIS*. (pp. 221-226).

Kumaraguru, P., & Cranor, L. F. (2005). Privacy indexes: a survey of Westin's studies (pp. 368-394). Carnegie Mellon University, School of Computer Science, Institute for Software Research International.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*, 540-563.

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication*, *8*(2), 291-301.

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media+ Society*, *4*(3), 2056305118784770.

Proctor, R. W., Ali, M. A., & Vu, K. P. L. (2008). Examining usability of web privacy policies. *International Journal of Human–Computer Interaction*, *24*(3), 307-328.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114.

Tsai, Y. S., Whitelock-Wainwright, A., & Gašević, D. (2020, March). The privacy paradox and its implications for learning analytics. *Proceedings of the Tenth International Conference on Learning Analytics & Knowledge* (pp. 230-239).

van Ooijen, I., Segijn, C. M., & Opree, S. J. (2022). Privacy Cynicism and its Role in Privacy Decision-Making. *Communication Research*, 00936502211060984.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7(6), 1.

Van Slyke, C., Parikh, M., Joseph, D., & Clary, W. G. (2021). Rational Ignorance: A Privacy Pre-Calculus, *Proceedings of the 16th Pre-ICIS Workshop on Information Security and Privacy*, Austin, TX.

Westin, A., & Harris Louis & Associates. (1991). Harris-Equifax Consumer Privacy Survey. Tech. rep., 1991. Conducted for Equifax Inc.

Wilson, S., Schaub, F., Dara, A. A., Liu, F., Cherivirala, S., Leon, P. G., ... & Sadeh, N. (2016, August). The creation and analysis of a website privacy policy corpus. In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)* (pp. 1330-1340).

Wirth, J., Maier, C., & Laumer, S. (2018). The influence of resignation on the privacy calculus in the context of social networking sites: an empirical analysis, *Proceedings of the Twenty-Sixth European Conference on Information Systems*, Portsmouth, UK.

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.