

Privacy, Vulnerability, and Willingness to share: An Empirical Investigation Using Latent Growth Curve Model

We are in the era of Internet of Things (IoT) with big data as one of its distinct features. As personal data being one source of big data, we can foresee that in the near future, the demand, supply and exchange of personal data would increase drastically. Despite the various benefits, personal data could also potentially bring about negative effects for firms and individuals; primarily associated with privacy issues. Thus, privacy has become increasingly important in order to harness the economic values of personal data in digital economy. In order to address privacy related issues, government and policy makers have entered this space through legislation for privacy protection such as EU GDPR. Technologies have been developed to tackle these issues. For example, Hub of All Things (HAT) is a personal data platform, which has taken the user-centric approach to privacy and implemented personal micro- server technology with the hope of empowering individuals to take charge of their personal data competently and also to benefit from their personal data with their privacy being protected.

Research has shown that perceived privacy is associated with individuals' willingness to share their data (Belanger et al, 2002), which is crucial for makes it a challenge for enterprises to leveraging benefits of from personal data. Perceived privacy is contextual and interactive depending on what to share and with whom to share the information (Dourish, et al, 2003). Thus, perceived privacy would change with time, evolution of the relationships with the data-exchange parties. Research has shown that consumer's concern for privacy is not absolute, as it often requires trade-off between privacy concerns and economic benefits (Kehr, et al, 2015). In some cases, we are relaxed about the scrutiny, i.e., we are willing to give up privacy in exchange for rather simple services. The key issue here is that making these trade-offs for information disclosure decision requires consumers to have the skill/capability to understand the implications of information sharing. When consumers lack the competency needed to make the judgment between trade-offs, they are deemed 'vulnerable' (Baker, et al, 2005). The perceived vulnerability would further compound their willingness to share information. Hence, vulnerability would be another key issue to be addressed as to protect consumers from the negative externalities of the personal data market while enabling them to benefit from the service offerings.

Despite technology and other methods aiming to enhance users perceived privacy, tackle vulnerability and consumer willingness to share, nonetheless, the challenge is how to measure the dynamics and change of individual perceived privacy, vulnerability and the effectiveness of these intervention methods for empowering privacy and reducing vulnerability and enhance consumers' willingness to share information. In this paper, we would contribute to gaining insights into these issues by examining the following research questions:

1. Does the perceived privacy for information sharing differ in accordance with their technical knowledge/skills for data?
2. To what extent do perceived privacy and vulnerability in particular data sharing change over time?
3. To what extent do individuals' willingness to sharing information change over time as their knowledge and competency level grows over time

Justification for the use of the HAT database is based on its richness as an incubator for a diverse set of applications that house information on various users that have varying degree of concerns over their privacy and perceived vulnerability. Anchoring on this database, we will embed an application wizard that voluntarily allows collection of primary information from HAT stakeholders. This is achieved by recruiting participants to get engaged in a longitudinal research by using 3-wave panel data. At the first wave, we could invite participants to sign up a HAT; provide participants with questionnaire to measure their perceived privacy, perceived vulnerability and willingness to share information; and also provide a reward depending on how much information they really share. At the second and third wave, we would provide participants with the same questionnaire to measure their perceived privacy, perceived vulnerability and willingness to share information; and also provide a reward depending on how much information they really share. We will take into account their different characteristics, such as experience and awareness on privacy issues, while expect to control for socio-economic factors that explain the differences among users from different countries.

The modelling approach that will be used for this study is the Latent Growth Curve model (LGCM), which would allow us to investigate the latent aspects of privacy, vulnerability and information sharing behaviour over time as manifested by their respective observed indicators. This method is particularly appropriate as it could structure for changes in growth of variables over time using a longitudinal data supported by HAT. The latent growth curve model will be analysed in two stages, i.e. an unconditional model in the first stage, and a second stage conditional model. The unconditional model measures a growth curve for a specific time frame as determined by the phenomena of incidence, and then fits the individual over repeated-measures data. The conditional model connects the intercept and the slope based on which of the study variables are influential predictors. We will then use a goodness-of-fit measure to ascertain the validity of the model.

The theoretical significance of the research is to capture the dynamics of privacy and vulnerability and their behavior change with the interventions such technology as the HAT. The empirical implications is that this model would potentially enable policy makers and firms to evaluate the effectiveness of their interventions of programs to improve individual privacy and reduce vulnerability of personal data. In addition, for firms, they can develop mechanisms to evaluate the changes of consumers' willingness to share their personal data over time and identify the key factors for

bringing about these changes and design business models to harness the economic values of personal data in a privacy protection manner.

References:

- Baker, S.M., Gentry, J.W. and Rittenburg, T.L., 2005. Building understanding of the domain of consumer vulnerability. *Journal of Macromarketing*, 25(2), pp.128-139.
- Belanger, F., Hiller, J.S. and Smith, W.J., 2002. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The journal of strategic Information Systems*, 11(3), pp.245-270.
- Kehr, F., Kowatsch, T., Wentzel, D. and Fleisch, E., 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6), pp.607-635.
- Palen, L. and Dourish, P., 2003, April. Unpacking privacy for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 129-136). ACM.