# Research on Criteria for Personal Information Collection Consent Based on Trust

Goo Yeon Lee
Dept. of Computer and Communication Eng.
Kangwon National University
Chuncheon-si, Gangwon-do, Korea
email: leegyeon@kangwon.ac.kr

Hwa Jong Kim
Dept. of Computer and Communication Eng.
Kangwon National University
Chuncheon-si, Gangwon-do, Korea
email: hjkim@kangwon.ac.kr

***Abstract*—In this paper, we study the criteria for determining whether to provide personal information to a service provider based on its trust. The study analyzes the relation between the service provider's trust, the profit gained from subscribing to the service, the expected loss of the potential personal information leakage or misuse, and the activation cost. The analyzed results will be useful for the development of an automated personal information consent algorithm in the future.**

***Keywords-trust; personal information; consent; collection.***

## I. INTRODUCTION AND RELATED WORK

Generally, when a user wants to use a specific service related to the individual, a personal information collection procedure is performed by the service provider. In case of offline, the consent process for collecting personal information is signed face-to-face. In the online case, the user understands the terms of processing personal information through a screen of a computer or a smart phone, and the consent or rejection indication thereof is performed. However, when we actually agree to the collection of personal information, we worry about whether our personal information may be misused later and some loss occurs.

In many cases, the confidence in a service provider is determined based on its reputation or the past experience of using other services from the provider. However, some users may consent without any prior knowledge of a service provider, which is recommended to avoid because there is a risk of personal information abuse such as voice phishing.

Recently, a lot of researches have been made to measure and utilize mutual or objective trust in the exchange of information between various entities on the Internet. If trusts from different entities on the Internet can be developed and quantified, these trusts can be used when providing personal information to service providers for using specific services.

There are many research and standardization efforts on trust. International Standardization of Trust Technology in ITU-T SG13 and ITU-T Y.3052 document [1] classify trust into direct trust such as belief, faith, confidence and dependence, and indirect trust, such as reputation, recommendation, expectation and experience. In addition, trust value evaluation methods based on knowledge, experience and reputation have been proposed [2][3] and several studies related to trust have been conducted [4]. However, it is considered that there has not been any research on the trust combined with the consent for providing personal information when joining services.

When a trust is applied to the service provider that collects personal information, the user can make a decision on whether to provide personal information based on the trust. However, trust cannot be 100% certain, so no matter how high the trust is, there is a possibility of personal information leakage and misuse. Therefore, there is a tradeoff between the benefit of using the service and the potential loss from personal information leakage and misuse. Accordingly, it is necessary to make an optimal decision to ensure that the benefit can be greater than the potential loss. In this study, we analyze the criteria for judging whether to provide personal information by quantifying the benefit obtained from the service and the risk of personal information exposure and abuse based on the trust of the service provider.

In this paper, we perform an analysis in Section 2 and discuss results in Section 3. Finally, we draw a conclusion in Section 4.

## II. ANALYSIS MODEL

In this section, we analyze the relation between the benefit from using the service and the potential loss due to the exposure or misuse of personal information based on the trust. The followings are definitions of parameters used in this section.

***T*** : It indicates the trust of a provider. It has a value between 0 and 1. A trust of 1 represents the case where the trust is 100%, and 0 represents the case where there is no trust at all. This value is estimated by a trust model. We expect that some trust rating companies like the existing credit rating companies will be formed and users may obtain the trust information of providers from the companies.

***R*** : It presents the risk to be taken by providing personal information. This can be expressed as a function of provider's trust. It has a value from 0 to 1, and has a value of 0 when there is no risk at all and a value of 1 when the risk is 100%.

***P*** : It represents the service profit that a user obtains from using the service. This value may be specified by a user, but a normal value can be recommended as the service is settled.

***L*** : It shows the expected loss if the user's personal information is exposed or misused. This value may be specified by a user, or may use the amount of the court's reimbursement decision for recent personal information leakage.

***C*** : It represents the activation cost. The user does not use the service immediately just because the service profit is greater than the expected loss. Basically, the net profit must be

 ISBN: 978-1-61208-760-3 

above the activation cost. This value is different depending on the user's disposition and situation.

We consider the risk $R$ for the service provider according to the trust($T$). If $T$ is 1, it has 100% confidence and $R$=0. And if $T$ is 0, it is 100% dangerous and $R$=1. In general, risk decreases sharply as trust increases from zero, and gradually decreases after some confidence. In other words, risk is convex down when trust changes from 0 to 1. There are many relations that satisfy these conditions, but we choose the following approach. The exponential function is suitable as a function that satisfies these characteristics. If the boundary condition of $R$ = 1 when $T$ = 0 and $R$ = 0 when $T$=1 is applied, we suggest the following relation.

$$R = \frac{e^{-AT} - e^{-A}}{1 - e^{-A}}, \quad (1)$$

where $A$ is a characteristic constant representing the confidence sensitivity. When $A$ is larger, the risk has smaller value even at the same trust value. On the contrary, when $A$ becomes small, it represents a situation of judicious judgment. In Figure 1, we give a graph of the relationship between $T$ and $R$ when $A$ is 1, 3 and 5. The measurement of $A$ value is outside the scope of this study, so it may be determined sociologically or economically. We expect that trust rating companies will assess the characteristics of a country or society to determine its confidence sensitivity and provide it to users.

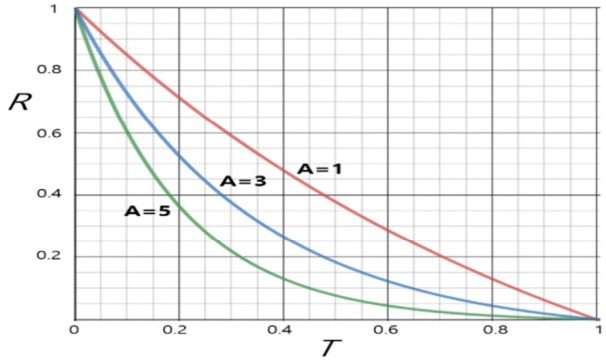


Figure 1. Relation between $T$ and $R$ when A=1, 3 and 5

The user subscribes to the service only when the net profit after subtracting the expected loss from the profit is greater than the activation cost. Here, we use the value of risk $R$ as the probability that personal information will be exposed or misused. Therefore, when the following formula is established, the user provides consent in the agreement procedure to the service provider.

$$P - L \cdot R \geq C \quad (2)$$

Substituting (1) into (2) gives the following equation:

$$P - L \cdot \frac{e^{-AT} - e^{-A}}{1 - e^{-A}} \geq C \quad (3)$$

Solving (3) with respect to $T$, we get

$$T \geq -\frac{1}{A} \ln \frac{(P-C)(1-e^{-A}) + Le^{-A}}{L} \quad (4)$$

## III. Results and Discussion

From (3) and (4), we have $P_{\min} = C + L$ when $T$=0 and $P_{\min} = C$ when $T$=1. That is, the value of $P$ is meaningful when it exists in the interval between $C$ and $C + L$. In Figure 2, we give the graph of minimum trust as $P$ varies when $C$ = 5000KRW(Korean won) and $L$ = 10000KRW. Parameter $A$ was assigned a value of 3.

When $P$=5000, the profit $P$ from signing up for the service is just equal to $C$ = 5000. In the case, there is no reason to join the service if there is any risk. That means the user can join only if there is no risk of personal information leakage or misuse. When $P$ = 15000, there remains 5000KRW even if 100% loss ($L$=10000) is assumed. In this case, even if there is a 100% loss of personal information leakage or abuse, motivation for signing up is sufficient. In addition, we can see that when $P$ = 6000, the minimum trust should be about 0.649. However, when $P$ = 11000, the customer will sign up for the service even if the trust is lowered to 0.161.

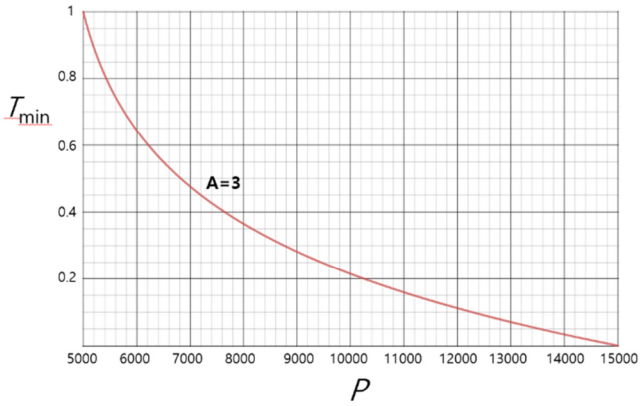


Figure 2. Minimum trust as $P$ varies when $C$ = 5000KRW, $L$ = 10000 KRW and $A$ =3

## IV. Conclusion

In this paper, we study the case where a user provides personal information to a service provider. In the study, we define the provider's risk based on its trust, and then derive the decision equation for the personal information collection consent by analyzing the profit gained when subscribing the service and the expected loss of the provider's personal information leakage or misuse. The analyzed results will be useful for the consent decision to provide personal information at the time of subscription.

## Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (Ministry of Science and ICT) (No.2018-0-00261, GDPR Compliant Personally Identifiable Information Management Technology for IoT Environment).

 ISBN: 978-1-61208-760-3 

## REFERENCES

[1] Telecommunication Standardization Sector of ITU, ITU-T Y.3052: Overview of trust provisioning in information and communication technology infrastructures and services, Mar. 2017. Online: https://www.itu.int/rec/T-REC-Y.3052/en [accessed Jan. 2020]

[2] N. B. Truong, T. Um, B. Zhou, and G. M. Lee, "Strengthening the Blockchain-Based Internet of Value with Trust," 2018 IEEE International Conference on Communications (ICC), 2018, pp.1-7.

[3] F. Alam and A. Paul, "A computational model for trust and reputation relationship in social network," 2016 International Conference on Recent Trends in Information Technology (ICRTIT), 2016, pp.1-6.

[4] M. Jäger, S. Nadschläger, and J. Küng, "Concepts for Trust Propagation in Knowledge Processing Systems - A Brief Introduction and Overview," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp.1502-1505.

 ISBN: 978-1-61208-760-3 