Perceived Responsibilities of Internet Users on Cybersecurity Issues

Extended Abstract

Daegon Cho
College of Business, KAIST
85 Hoegi-ro Dongdaemun-gu, Seoul Korea
dgcho@business.kaist.ac.kr

Jaeung Sim
College of Business, KAIST
85 Hoegi-ro Dongdaemun-gu, Seoul Korea
jaeung@business.kaist.ac.kr

Jae Kyu Lee
College of Business, KAIST, Yonsei University
85 Hoegi-ro Dongdaemun-gu, Seoul Korea
jklee@business.kaist.ac.kr

Keywords

Perceived risk, Cybersecurity, Responsibility, Bright Internet Principles

Perceived Responsibilities of Internet Users on Cybersecurity Issues

In 2013, Edward J. Snowden's disclosure of the government's vast surveillance programs provoked a controversial public debate on the trade-offs between security against potential terror and protection of personal privacy (Shear et al. 2016; Barret and Wakabayashi 2016). In a similar vein, Ackerman (2006) argues that the terror triggers public outrage and allows politicians to pass restrictive legislation to strengthen the social security system. However, Dragu (2011) insisted that privacy and protection from terrorism are not in conflict; that is, reducing security level does not necessarily increase the level of privacy protection. In 2016, while the Federal Bureau of Investigation (FBI) asked Apple Inc. to unlock the terrorist's iPhone, the CEO of Apple, Tim Cook, claimed it could be perilous regarding privacy of personal information. On this issue, The Wall Street Journal and NBC asked people, "whether the U.S. would not go far enough in monitoring terror suspects' communications, or whether the government would go too far and violate the privacy of its citizens" (Barrett 2016). The survey result showed that 47% of respondents was in favor of the government policy, and 44% was against the policy, which indicates that the debate between the fear of terrorism and public concern about digital privacy is universal. As cybercrimes have consistently increased and diversified over time, understanding the risk perception and experience of the general public may be of key importance in establishing appropriate preventive strategies.

In this context, this study examines perceptions and responsibilities of Internet users on cybersecurity issues from multi-year surveys. On one hand, in 2015, we conducted a nationwide survey in South by which we ask the needs for a new Internet regime on the basis of the Bright Internet principles suggested by Lee (2015). Most previous studies generally assumed that the fundamental mechanism in terms of Internet security is a given condition, and the scope of their studies cover a fraction of individuals or firms. However, in practice, an increasing number of Internet-based organizations and private firms still have difficulties dealing with individual data and the security of it. In this regard, a fundamental shift of principles governing cyber security and privacy issues may need to be considered, and Lee (2015) proposed the Bright ICT Initiative.

As a gist of the initiative, four Bright Internet Principles – i) origin responsibility, ii) deliverer responsibility, iii) rule-based digital search warrants, and iv) traceable anonymity – are proposed as guiding principles to essentially change the current cyber security system. We conjecture that the degree of preferences for the suggested principles may be related to each individual's perception and experiences from their own activities on the Internet. Thus, we conduct a nationwide survey in South Korea to investigate citizens' awareness and understanding of cyber security. In other words, the first study aims at encapsulating the main results of the survey and presenting preliminary results of the relationship between the citizens' awareness of the cyber security and their desire of the new Internet regime. Findings from 1,027 respondents suggest that most Internet users perceive that the cyberspace is in danger with high risks generated by various cybercrimes. Therefore, they express the strong necessity of implementing the principles, and positive assessments on Bright Internet principles.

In particular, to reduce cybercrimes, users believe that the root causes need to be concerned regardless of technical limitations of detecting offenders. This perspective is associated with the origin responsibility principle suggested by Lee (2015). We also find that citizens' perceived risks and experiences of risk factors on the Internet affect their desire for new Internet regime. In this survey, we find salient evidence of Internet users' perceptions and needs for the new Internet paradigm. In line with this observation, Lee et al. (2017) examine the need for a prescriptive

design for the global scale information infrastructure, encompassing the constructs of technologies, policies and global collaborations.

On the other hand, from the different angle, we conduct an additional survey with a special emphasis on the responsibility chain. Specifically, we first give respondents problematic situations including email phishing, malware diffusion via emails, or email spoofing. We allow them to acknowledge relevant stakeholders, such as an email sender (origin), an email receiver (destination), email service providers of the sender and the receiver (e.g., Google Gmail), and Internet network provider (e.g., Comcast). We then ask them to assign the weight of responsibilities of the given cybersecurity problem. By doing this, we expect to acknowledge how Internet users define where the matter of responsibility lies. We also ask them how much we can detect the origin's identity in the given Internet regime and whether it is necessary to increase the likelihood of identifiability. This survey is being conducted in late November 2017, and the preliminary findings will be shared at Bright Internet Global Summit 2017.

In summary, these two complementary surveys in South Korea examine how Internet users recognize risk factors on the Internet and what can be the possible solution to mitigate the prevailing cybercrimes. We also investigate perceived responsibilities of Internet users on prevalent cybersecurity issues in different approaches. As a consequence, we explore the necessity of the new Internet regime and the desirable directions of the future Internet infrastructure. In this regard, this study may provide important policy implications of global collaboration on cybersecurity issues.

References

Ackerman, B., 2006. *Before the Next Attack: Preserving Civil Liberties in the Age of Terrorism*, New Haven, CT: Yale University Press.

Barrett, D. and Wakabayashi, D., 2016, "U.S. and Apple Dig In for Court Fight Over Encryption," *The Wall Street Journal*.

Barrett, D., 2016, "Americans Divided Over Apple's Phone Privacy Fight, WSJ/NBC Poll Shows," *The Wall Street Journal*.

Dragu, T., 2011. "There a Trade-off between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention," *The American Political Science Review* 105(1): 64-78.

Lee, J. K., 2015. Research Framework for AIS Grand Vision of the Bright ICT Initiative, *MIS Quarterly* (39:2) Guest Editorial.

Lee, J. K., D. Cho, and G.G. Lim. 2017. "Design and Validation of the Bright Internet," *Journal of the Association for Information Systems. forthcoming*.

Shear, M. D., Sanger, D. E. and Benner, K. 2016. "In the Apple Case, a Debate Over Data Hits Home," *New York Times*.