Social Consensus on Privacy Level

Gongpil Choi

Leverage of data is the core competitiveness for future growth. Big data and AI obviously have ensconced as indispensable tools for creating new values. But look where we are at now, who have been standing at the forefront of IT powerhouses. People take sides, raising their voice for and against privacy protection, which is perceived to be conflicting with data application. True, we are living in a digital age, but broad consensus on privacy level will never be made if data owners continue to feel insecure. Therefore, we definitely need a set of guidelines and social agreement on how to deal with sensitive information and privacy. However, drawing this up is not easy in Korea due to the fragmented legacy system. Advanced laws and regulation system such as the GDPR (General Data Protection Regulation) should be established, but the existing governance structure are far behind the current paradigm. Even just putting together the opinions on data privacy level among the social members is a heavy going.

Privacy level in digital space that requires to be agreed upon will vary from case to case. In this era where information is money, digital cash would be an appropriate example to extend the discussion. Digital cash is a product that embodies social consensus on privacy with encryption technology. Central bank cash has been providing basic privacy to the public. It has been misused for money laundering and tax evasion of the underground economy on the one hand, but is still a store of value that enables uninterrupted autonomous transaction.

Even in the future digital world, individuals ought to have the right to freely use cash. That is to say, money that guarantees anonymity is more than just a matter of convenience: It is the basic right of human beings. The problem is, how do we decide the privacy level of digital cash? If the protection level is too high, our society will be under social control; while too much of a privacy will make it hard for the community to build up a shared value. In the end, it is all about data privacy that leads us to the future digital life.

Thus, we must prepare for the future ecosystem by reaching a social concurrence on privacy level. We should first lay a new foundation of trust to cope with the digital environment, where privacy is more concerned than the past times that totally depended on the choice of legal
subjects. We could not just uniformly regulate all transaction anonymity of individuals under the name of uncertainty. Rather, we should seek a way to overcome the conflict between security and privacy by technology advancement.

The regulation of privacy should be differentiated according to sector and desired level. Systematically vulnerable sectors or individuals who want more security should take the additional burden. Moreover, it is preferable to only provide essential information for electronic commerce under the scheme in which the choice of personal information is attributed to the provider. In addition, virtual identity in virtual space should be more broadly accepted. Also, the collected and utilized information should be discarded after a certain period of time or should be subject to prudential regulations regarding data storage, processing, and sales. Last but not least, relative authorities should ensure a certain level of privacy option to everyone regardless of their income and background, while creating an inclusive and open ecosystem to protect the rights of the digitally weak.