JoongAng Daily
English Joongangilbo - IHT Partner

Print Page
Print

The significance of data protection in Korea

February 19, 2011


Park Whon-il

Korea has the highest distribution rate of Internet broadband networks in the world. But this has a down side - it increases the chance of data breach incidents as resident registration (RR) numbers are generally used online.

A new version of the Data Protection Act is currently before the National Assembly.

Professor Park Whon-il co-wrote an article with Graham Greenleaf, a professor at the University of New South Wales, Australia, about the need for data protection reforms.

The article, titled “Korean data protection reforms - More needed?”, will be published in this month’s issue of Privacy Laws & Business International Report.

Park, an associate law professor at Kyung Hee University, is the only Korean who has translated into English the current private sector data protection legislation and its legal implications.

In a recent interview, Park discussed some changes that should be made.

He describes Korea as having a 15-year history of data protection legislation, which is longer than any other Asia-Pacific jurisdictions except for Australia and New Zealand.

Park cites an example from earlier research regarding privacy concerns.

“In February 2008, an unidentified hacker with an overseas Internet

Protocol [IP] address broke into the Web site Auction, Korea's largest e-marketplace," he said. "The personal data of 10.8 million users were apparently leaked out of the country, raising privacy concerns."

According to Park, personal information is defined as the data of a living person such as character, voice, sound and image.

Due to technological advances, this has been extended to include data such as e-mail addresses, credit card numbers and log files.

This increases the vulnerability of cyberspace users, and Park described the use of RR numbers as "open sesame."

"Every door is opened with the RR number. So groups like Chinese hackers or North Korean espionage [agents] use RR numbers to [get at] the Korean data system," he said.

Though people have demanded a response from the government, Korea's private sector law is the strictest set of requirements in the Asia-Pacific region.

Businesses can only use personal information collected for the purposes stated at the time of collection. Where this is breached, the victim may seek pecuniary compensation.

"For example, one female patient underwent a plastic surgery operation," Park said. "And the clinic posted the movie of the patient's operation on its Web site without her consent, so was ordered to pay 4 million won [$3,593]."

Although there is a proposal for a newer version of data protection legislation, Park said it was uncertain when it would pass.

"Korean government officials were encouraged by the successful G-20 Summit last November," he said. "They are eager to demonstrate this draft framework act is advanced in view of the Asia-Pacific Economic Cooperation [APEC] Privacy Framework as well as the EU Data Protection Directive.

"The ruling party and opposition have agreed on the big issues of the new Data Protection Act, but it seems like they need some explosive incidents, such as a massive data leak ... to propel the bill."

Park said the public and private sector are currently governed by separate legislation.

“When Korea wanted to be admitted to the Organization for Economic Cooperation and Development [OECD],” he said, “the Korean government had to make OECD-level data protection in the public sector, which was later applied to data protection in the private sector as well.”

The proposed framework act seeks to regulate data protection in both the public and private sector.

Park said another hot issue is making an independent supervisory regulator for data protection.

“Koreans regard data protection as a symbol of democratization in society, and so far the politicians have been struggling to make an independent watchdog,” he said.

The supervisory watchdog as of date is under two governmental departments: the Ministry of Government Administration and Home Affairs for the public sector, and the Ministry of Information and Communication for the private sector.

Park also mentioned that neither the private nor the public sector acts yet include provisions for data breach notification.

By Joni Sham Intern reporter [jsha3324@uni.sydney.edu.au]

Print