PAUL HASTINGS
PH PERSPECTIVES

Privacy and Security Law: What Korean Companies Need to Know

By Paul M. Schwartz

Personal data is the gold of the information economy – a new profit source for companies seeking to know more about their customers and better meet their needs. This is especially true for Korean companies, who are leading manufacturers of world-class phones, refrigerators, automobiles, and other products. Each year, more of their products are smart devices that collect information about the end users. As a result, the legal and business demands of privacy-sensitive and security-aware foreign markets should be a priority for Korean businesses.

The critical need is to act now to design products that are privacy- and security-compliant and to plan ahead to capture the value of personal information in evolving business models. For Korean companies, the key task is to recognize that personal data offers not only compliance risks but also important business opportunities. To provide context for this changing environment, Paul Hastings special advisor **Paul Schwartz** shares his perspective on the issues Korean companies must consider as they navigate the U.S. and EU legal landscape:

How do devices and appliances connect to the Internet of Things?

Automobiles, phones, refrigerators, and other devices and appliances now collect information about users' habits and preferences. This information is also increasingly given unique identification numbers and connected digitally using a variety of protocols and applications. This trend of networked smart devices is called the "Internet of Things." This development raises significant privacy and security issues for a wide variety of products that were once unproblematic in this regard.

Already, automobiles are sophisticated "computers on wheels" that are controlled by dozens of mini-computers. These digital processing units control everything from steering and braking to emissions. They also manage the deployment of critical safety systems like airbags. Depending on the manufacturer and model, an automobile may use computers to supply consumers with entertainment, travel options, mapping information, and sensors that allow a driver to remotely access a car's digital information via a smartphone. These data are highly valuable; the manufacturer and other parties can use them to meet the driver's needs for warranty service, repairs, personalized travel tips, and a host of other matters. A similar development is occurring for a wide range of devices and appliances as the information generated by their use becomes an attractive source of new business profits.

What are the challenges and opportunities for Korean companies as they design and market ever-more sophisticated "smart" products?

The challenge for Korean companies is a double one. First, they must think ahead in designing products that meet the requirements of the privacy and security-conscious countries where they sell their wares. "Privacy-by-design" is a key concept in this regard: it means that information privacy as well as security requirements should be built into software and hardware as part of the planning process. This approach to compliance creates an important business advantage in today's world, where business-to-business contracts increasingly demand the highest level of privacy and security from manufacturers and vendors. Privacy-by-design also reduces compliance costs by determining in advance the most effective ways to fulfill legal requirements and meet customer expectations.

Second, Korean companies must recognize that their future increasingly involves the collection, use, and transfer of personal information. This offers a new path for developing and marketing products and services to be sold to customers. Rather than acting exclusively as original equipment manufacturers that let other parties have access to personal data, in the future Korean companies will seek to draw on personal information to find out more about their customers, to better meet their needs, and to develop new products and services. But such future profitable uses of personal information require compliance with the law of the United States and European Union.

What is the legal framework covering information privacy in the U.S.?

A patchwork of information privacy law exists in the U.S. Where nations in the EU have long enacted omnibus information privacy laws, the U.S. has promulgated only sectoral laws. An omnibus privacy law typically sweeps in the public and private sectors and regulates all sectors of information use. In contrast to an omnibus law, a sectoral law regulates only a specific context of information use.

As examples of sectoral privacy laws, the Fair Credit Reporting Act (1970) contains rules for the use of credit reports, and the Graham-Leach-Bliley Act (1999) establishes rules for financial institutions concerning the use of "non-public personal information." Beyond the sectoral nature of U.S. privacy law, there are three additional dimensions to privacy law in the U.S. These aspects relate to federalism, the role of the Federal Trade Commission (FTC), and the risk of class action lawsuits.

In the U.S., there is a dual federal-state system of lawmaking. As a result, a state such as California can lead the way with important privacy statutes. California now has significant laws that require data breach notification, secure data disposal, and the posting of certain mandated information on websites. These requirements are placed on entities wherever they are located in the world; the jurisdictional trigger is that the organization collects the personal information of California residents.

As a further important dimension of U.S. privacy law, the FTC has developed a "common law" of information privacy law in the U.S. The FTC draws on enforcement power granted in the Federal Trade Act, established in specific privacy legislation, and provided by the Safe Harbor agreement with the EU. The FTC has acted to stop deceptive and unfair practices and identified a range of inadequate security practices. Its many settlements of enforcement actions have frequently included large fines, such as Apple's US$32.5 million privacy settlement in 2014 and Google's US$17 million and US$22.5 million settlements in 2013 and 2012, respectively.

Finally, class action privacy lawsuits are an omnipresent reality in the U.S. On June 13, 2014, for example, Sony settled for US$15 million a class action suit over a massive data breach for PlayStation users. Consumers may sue companies pursuant to explicit private rights of actions in certain privacy statutes, or under the broad authority contained in state consumer protection laws, such as California's Unfair Competition Act. Pursuant to the California ban on unfair competition, individuals and government entities are able to seek judicial remedies, including injunctions, for any unlawful, unfair or fraudulent business act or practice.

How do data protection laws differ in the EU?

EU information privacy law, traditionally called "data protection law," takes an omnibus approach. The EU's national data protection laws are also all "harmonized" to meet the requirements of the European Data Protection Directive (1995). Nonetheless, important distinctions remain among EU Member States, which makes compliance for international companies a complex legal challenge.

The next step for the EU is enactment of its Data Protection Regulation, which was released in 2012. The Data Protection Regulation will be directly binding on all Member Nations. The current draft increases the rights granted to individual citizens of Member Nations beyond those in the Directive. For example, it grants a "right of erasure," that is an interest in deleting old personal information.

One thing that will not change, however, under the Regulation concerns the strict rules for transfer of personal data outside of the EU. Like the Directive, the Proposed Data Protection Regulation prohibits transfers of personal data outside the EU to third countries that do not have "adequate" data protection. The U.S. and Korea alike are not considered to meet this standard. Fortunately, there are a number of mechanisms for transfers of personal data outside of the EU. For the U.S., there is the Safe Harbor Agreement. For the U.S. and Korea, there is the possibility of using Model Contractual Clauses and Binding Corporate rules.

For more information, please contact:

Paul Schwartz
San Francisco
+1.415.856.7090
paulschwartz@paulhastings.com

Jong Han Kim
Seoul
+82.2.6321.3801
jonghankim@paulhastings.com

Paul Hastings is a global law firm with a strong presence in Asia, Europe, Latin America, and the United States. The firm has one of the largest full-service, multi-jurisdictional legal practices in Asia, with locations in Beijing, Hong Kong, Seoul, Shanghai, and Tokyo.