New Privacy Guidelines Now Effective in South Korea: Online Customized Ads; Smartphone App Access Rights

JULY 26, 2017

Two new privacy guidelines are now effective in South Korea. Earlier this year, the Korea Communications Commission (KCC) published "Privacy Guidelines for Online Customized Ads" (Korean language link) and a "Privacy Guide for Smartphone App Access Rights." The KCC indicated that both sets of guidelines would take effect in July, after which the KCC would begin checking whether companies have implemented appropriate measures to comply with South Korea's privacy laws and regulations. Companies that engage in online customized advertising or participate in the mobile app ecosystem in South Korea—including publishers, third-party service providers, operating system providers, smartphone manufacturers, and app market operators—should take steps to ensure compliance with South Korea's new privacy guidelines.

Privacy Guidelines for Online Customized Ads

In February, the KCC issued its "Privacy Guidelines for Online Customized Ads" (the "Guidelines") that describe the steps that companies must take when engaging in online customized advertising in South Korea. The Guidelines define "**online customized advertisements**" as advertisements that are customized to the user after analyzing and inferring the user's interest, preferences, and inclination by processing "**behavior information**," which is defined as online activity information that can identify and analyze the user's interests, preferences, and tendencies, such as history of website visits and history of application usage. Importantly, South Korea's Guidelines apply to behavior information collected and used in both **websites *and* mobile apps**.

The Guidelines describe various requirements applicable to both "**advertisers**" (defined as companies that collect behavior information through online media, such as their own or third-party websites and apps, and transmits online customized advertisements) and "**media businesses**" (defined as businesses that allow the collection of behavior information through online media, such as their websites and apps). In this regard, the Guidelines are very similar to the notice-and-choice framework established in the United States under the Federal Trade Commission's 2009 Staff Report on Self-Regulatory Principles for Online Behavioral Advertising and the Digital Advertising Alliance's (DAA) Self-Regulatory Principles for Online Behavioral Advertising and related guidance. The Guidelines recommend that advertisers and media businesses:

- **Provide information to users in a privacy policy, including**: (1) the **types of behavior information** collected or transferred to third parties; (2) the **purpose** of collecting such information; (3) the **methods** of information collection; (4) **how to opt out or exercise other choices**; (5) **data retention and use periods and any subsequent processing**; (6) **how consumers can seek redress**; and (6) to the extent that a company allows third parties to collect behavior information through its websites or mobile apps or otherwise provides information to third parties, **the names of the third-party companies collecting, receiving, or processing behavior information**;
- **Install icons in or around online customized ads** that can be easily identified by users (such as the DAA's Advertising Options icon);
- **Provide a means for users to opt out or exercise other choices**, including:
  - Providing a **direct means for users to opt-out**, either through the advertisements themselves or by providing opt-out links;
  - By **describing how users can control online customized ads through the user's browser or mobile device settings**, such as by deleting or blocking cookies or setting ad preferences on a mobile device;
  - **Providing links and explanations to industry self-regulatory opt-out pages** where consumers can block online customized ads, such as the opt-out pages provided by the DAA or Network Advertising Initiative (NAI);
- **Minimize information collection** to the minimum amount necessary;
- **Do not collect, use, or analyze sensitive behavior information—such as an individual's thoughts, beliefs, family and friendship relationships, academic background, or illness—without the prior consent of the user**;
- **Do not collect behavior information from children under 14 years old**;
- **Obtain prior consent from users before combining behavior information with personally-identifiable information**, and only after clearly informing the user of the fact, the purposes of use, types of information combined, and retention periods;
- **Implement technical and administrative safeguards to protect users' behavior information** against unauthorized use, disclosure, or fraud, and **retain data only for the minimum amount of time necessary** to achieve the company's purposes, unless otherwise required by law;
- **Take steps to increase consumer awareness of online customized advertising and implement processes to address user inquiries, suspend campaigns, provide damages or other relief, and resolve claims of infringement of users' personal information**.

The Guidelines also provide detailed instructions for consumers to help them understand how users can exercise control over online customized advertising.

Privacy Guide for Smartphone App Access Rights

In March, the KCC also issued a "Privacy Guide for Smartphone App Access Rights" (the "Guide"), which describes how to comply with South Korean privacy laws and regulations when collecting information through smartphone mobile apps. In its press release, the KCC stated that the

amended Act on the Promotion of Information and Communications Network Utilisation and Information Protection ("the Network Act") and a related enforcement decree from March 23, 2017, requires that app service providers distinguish "optional" from "necessary" access rights for smartphone apps, notify users of this information, and obtain users' consent to access personal data stored on users' smartphones. The KCC indicated that its Guide was intended to prevent any confusion regarding implementation and to promote an accurate understanding of the law.

The Guide **applies to all actors in the mobile app ecosystem that operate on smartphones and tablet PCs with mobile communications capabilities**, including operating system providers, smartphone manufacturers, app market operators, and app service providers. However, the KCC indicated that its Guide **does not apply to the collection of information through devices that use Bluetooth, WiFi, or tethering functions without utilizing mobile communications networks**.

In terms of substantive requirements, the Guide imposes different compliance measures on various actors in the ecosystem, as follows:

- **App service providers**: (1) notify users of necessary and/or optional access rights; and (2) implement a process of notifying users and obtaining consent through the operating system's features. Importantly, the guide emphasizes that app service providers should: (a) distinguish between necessary and optional access rights; (b) clearly inform users about the categories and reasons that access rights are needed; and (c) explain how to procure user consent for access rights.
- **Operating system providers**: (1) provide features for obtaining consent and withdrawing consent; and (2) prepare and release standards governing access rights and security measures.
- **Smartphone manufacturers**: install operating systems on smartphones that allow users to provide or withdraw consent for access rights.
- **App developers**: implement settings that allow users to provide or withdraw consent for access rights during the process of developing and distributing apps, in a manner appropriate to the smartphone and smartphone operating system's environment.
- **App market operators**: (1) provide a space for notices about access rights; and (2) operate a system to monitor access rights.
- **Users**: after confirming the content of the notice regarding access rights, grant consent, or withdraw consent at a later time.

The KCC indicated in its press release that "[s]tarting in July 2017, the KCC will begin checking whether providers have implemented appropriate access measures and if they are complying with regulations."

Implication for Businesses

South Korea's data protection laws and regulations impose strict requirements on companies operating in South Korea. Accordingly, companies that expand into South Korea and other emerging markets should exercise caution and ensure that they comply with local laws and regulatory guidance, such as South Korea's new guidelines applicable to online customized advertising and

smartphone app access rights. The KCC has indicated that it will begin enforcing the new guidelines this month to ensure that companies comply with applicable laws and regulations.