NEWSLETTER
LIFANG & PARTNERS 立方观评
关注更多精彩内容
No.233
2021.04

Weekly Cybersecurity and Data Protection Review No.53

By Lifang & Partners

Domestic News

MIIT Seeks Advice on the Interim Regulations on the Management of Personal Information Protection for Mobile Internet Applications

MIIT Publishes the Proportions of Problematic Applications on the App Platform

TC260 Seeks Advice on 3 Recommended National Standards

LAC: Strict Legal Responsibility to be Set in Personal Information Protection Law

SPP Publishes Typical Cases of Public Interest Litigation Regarding Personal Information Protection

Ningbo AMR Fines 3 Real Estate Companies CNY 750,000 for Improperly Using Facial Recognition System

Overseas News

EDPB Publishes Final Version of Guidelines on Targeting of Social Media Users

EU Commission Proposes a Regulation on Artificial Intelligence

EU to Boost Cybersecurity Competence Centre

Domestic News

MIIT Seeks Advice on the Interim Regulations on the Management of Personal Information Protection for Mobile Internet Applications

On April 26, 2021, in order to strengthen the personal information protection collected by mobile Internet Applications and standardize the personal information processing activities of the relevant Apps, the Ministry of Industry and Information Technology ("**MIIT**") issued the *Interim Regulations on the Management of Personal Information Protection for Mobile Internet Applications (Exposure Draft)* and sought advice publicly. The deadline for advice submission is May 26. The exposure draft stipulates that, when an App processes personal information, the providers should follow the minimum necessary principle, and if the users refuse to authorize the unnecessary information, the providers must not force the users to exit or close the App; when processing sensitive personal information such as personal biometrics data, medical health, personal locations, etc., users should be informed separately and the providers may only process sensitive personal information after they obtain consent. (More)

MIIT Publishes the Proportions of Problematic Applications on the App Platform

On April 23, 2021, MIIT issued a statement, stating that during the first quarter inspection of 2021, the respective proportions of problematic Apps in Tencent App Store, Xiaomi App Store, OPPO App Store, Huawei App Market, and Vivo App Store were 14.22%, 13.81%, 12.80%, 11.37% and 11.17%. There were problems like failing to review the Apps in the App store according to the rules, failing to solve the problems already exists, inaccurate registration and verification of the information of App developers and operators, and misleading users to download, etc. MIIT has urged the relevant platform companies to carry out comprehensive rectification and strictly fulfill the company responsibilities. Meanwhile, MIIT also published the latest batch of problematic App lists, and required that the listed 138 Apps to be rectified completely before April 29. (More)

TC260 Seeks Advice on 3 Recommended National Standards

On April 23, 2021, the National Information Security Standardization Technical Committee ("**TC260**") issued an announcement, seeking for public advice on the recommended national standard: *Information Security Technology — Security Requirements of Face Recognition Data*. The deadline is June 22. Furthermore, on April 19, TC260 also sought advice on another two recommended national standards: *Information Security Technology — Personal Information Security Measurement and Evaluation Specification in Mobile Internet Applications* and *Information Security Technology — Guidelines for SDK Security in Mobile Internet Applications*.The deadline for these two standards is June 18. (More)

LAC: Strict Legal Responsibility to be Set in Personal Information Protection Law

On April 22, 2021, the spokeperson of the Legislative Affairs Commission ("**LAC**") attended a news hearing and introduced the draft of *Personal Information Protection Law*. According to the introduction, the draft will: further perfect the system regulations in the field of personal information protection, and establish rules for processing personal information, which are based on the "notification - authorization" principle; set up a special section to impose stricter restriction on processing sensitive personal information, and stipulates that sensitive personal information can only be processed when the processor

has a specific purpose and be with sufficient necessity, prior separate consent or written consent of the individual should be obtained and prior risk assessment should be carried out; clarify the rights of individuals in the processing of personal information activities, such as the right to know, the right to inquire, and the right to delete, etc., and strengthen the obligations of compliance management and of protecting personal information security of personal information processors. The draft will be submitted to the Standing Committee of the National People's Congress for review on April 26. (More)

SPP Publishes Typical Cases of Public Interest Litigation Regarding Personal Information Protection

On April 22, 2021, the Supreme People's Procuratorate ("**SPP**") published 11 typical cases of public interest litigation regarding personal information protection by procuratorial organs. Among the 11 public interest litigation cases, the administrative cases mainly involved personal information regulation by administrative agencies, government information disclosure issues, and private companies' disclosure of personal information; the civil cases mainly involved Internet companies' illegal collection of personal information and consumer fraud; and the criminal and incidental civil cases mainly involved illegal acquisition and trading of personal information (in such cases, the network operator, as a co-defendant, is required to bear the responsibility for public damages together with the actor). It is reported that in September 2020, the SPP issued the *Guiding Opinions on Actively and Steadily Expanding the Scope of Public Interest Litigation Cases*, in which the protection of personal information is listed as a focus of cyber infringement cases. (More)

Ningbo AMR Fines 3 Real Estate Companies CNY 750,000 for Improperly Using Facial Recognition System

On April 19, 2021, Ningbo Municipal Administration for Market Regulation ("**Ningbo AMR**") issued a statement, stated that it fined Ningbo Baoli Industrial Investment Co., Ltd. CNY 250,000, according to the *Measures for Penalties Against Infringement upon Consumers' Rights and Interests* and *Law on Safeguarding the Consumer Rights and Interests*, for infringing consumers' personal information right. Previously, on April 14 and April 15, there were another two real estate companies fined for the same reason for CNY 250,000 respectively. According to investigation, the three companies all have installed and used facial capture systems at the entrance of their sales offices to automatically capture and store the facial biometrics information of all visiting customers, so that they could compare with the biometrics information of the customers introduced by distributors. Once there is a match, the companies will pay commission to the distributors. Although two of the companies claimed that they had posted monitor collection marks at the entrance of the sales offices, Ningbo AMR rejected the defense and still concluded that it constituted an infringement of consumers' legally protected personal information rights. (More)

Overseas News

EDPB Publishes Final Version of Guidelines on Targeting of Social Media Users

On April 22, 2021, the European Data Protection Board ("**EDPB**") published the final version of its guidelines on the targeting of social media users which were adopted on 13 April 2021. In particular, the guidelines aim to clarify the roles and responsibilities of social media providers and targeters. As

such, the guidelines outline the potential risks to the rights and freedoms of individuals posed by the processing of personal data and identify the main actors and their roles. Furthermore, the guidelines seek to address the application of key data protection requirements, including lawfulness, transparency, and Data Protection Impact Assessments, as well as outline the key elements of arrangements between social media providers and the targeters. (More)

EU Commission Proposes a Regulation on Artificial Intelligence

On April 21, 2021, the European Commission proposed the first ever legal framework on AI: Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence. The specific objectives of the proposals are: to ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values and to ensure legal certainty to facilitate investment and innovation in AI, etc. To achieve those objectives, the proposal presents a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked to AI. The proposal also sets harmonized rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach, and lays down a solid risk methodology to define "high-risk" AI systems that pose significant risks to the health and safety or fundamental rights of persons. (More)

EU to Boost Cybersecurity Competence Centre

On April 20, 2021, the EU Council adopted the regulation establishing a Cybersecurity Competence Centre and the network, which will be followed by a final adoption by the European Parliament. The EU is set to boost the security of the internet and other critical network and information systems by establishing the Centre to pool investment in cybersecurity research, technology and industrial development. This "European Cybersecurity Industrial, Technology and Research Competence Centre" will work together with a network of national coordination centres designated by member states. The Centre will also bring together the main European stakeholders, including industry, academic and research organisations and other relevant civil society associations, to form a cybersecurity competence community, in order to enhance and spread cybersecurity expertise across the EU. (More)

Subscribe to our WeChat community

Beijing | Shanghai | Wuhan | Guangzhou | Shenzhen | Korea

www.lifanglaw.com
Email：info@lifanglaw.com
Tel：+8610 64096099
Fax：+8610 64096260/64096261