JUNHE BULLETIN

January16, 2020

NETWORK SECURITY AND PERSONAL INFORMATION PROTECTION LAW

Stricter Law Enforcement on the Collection of Personal Information by Apps; Highlights in Compliance

Two years have passed since *Cybersecurity Law* came in to effect. The rules and regulations on cyber security and information protection, as well as their enforcement, have become increasingly thorough. Apps are a potential disaster area, particularly when App operators over collect personal information, and this is why regulators have reinforced the regulation of Apps by promulgating detailed requirements. They have increased evaluations and made various orders, which are summarized as follows:

1. Rules and Regulations

In addition to *Cybersecurity Law* and other applicable national standards, in 2019, the Cyberspace Administration of China ("**CAC**"), the Ministry of Industry and Information Technology ("**MIIT**"), the Ministry of Public Security ("**MPS**") and the State Administration for Market Regulation ("**SAMR**") (hereinafter collectively referred to as the "**Four Administrations**") promulgated the following regulations (or drafts) specific to personal information collection and use in the field of Apps:

(1) *Circular concerning Special Campaigns against the Illegal Collection and Use of Personal Information by Apps*[1];

(2) *Circular concerning App Security Certification*[2];

(3) *Guidelines for Self-Examination of Apps on the Illegal Use of Personal Information*[3];

(4) *Rules on the Determination of Illegal Collection and Use of Personal Information by Apps*[4];

(5) *Information Security Technology --- Basic Rules on Personal Information Collection by Mobile Internet Applications (Apps) (Draft)*[5].

2. Status of Law Enforcement

The Four Administrations jointly or individually

[1] http://www.cac.gov.cn/2019-05/23/c_1124532020.htm
[2] http://www.gov.cn/xinwen/2019-03/15/content_5373928.htm
[3] https://mp.weixin.qq.com/s/u2XZn02SJkOvzeNSdzJiEA
[4] http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm
[5] https://mp.weixin.qq.com/s/y8EUsg9-vDMMinVuHR2ZEA

carried out a series of law enforcement campaigns for personal information protection during the period from January to December of 2019. For example:

(1) The Four Administrations carried out special campaigns against the illegal collection and use of personal information by Apps, established special App campaign committees, provided channels for reporting the illegal collection and use of personal information, evaluated hundreds of Apps, and in serious cases ordered the non-compliant Apps to make corrections[6];

(2) In the first quarter of 2019, MIIT organized a spot check on 106 Internet services provided by 100 Internet enterprises, and ordered the relevant enterprises to correct their failure to publish rules on the collection and use of users' personal information, their failure to provide channels for users to access and revise information, and their failure to provide functions for users to cancel their accounts, etc.[7];

(3) In March, 2019, SAMR carried out a campaign called 'To Protect Consumers' --- A Special Law Enforcement Campaign against the Illegal Infringement of Consumers' Personal Information, with a focus on the illegal infringement of consumers' personal information in the field of consumption[8];

(4) In 2019, MIIT initiated the 'Special Campaign against the Infringement of Users' Rights by Apps' [9] and other campaigns to crack down on the illegal collection of personal information, the illegal use of personal information, the unreasonable request for access from users, the creation of obstacles to prevent account cancellation, and other misconduct, by Apps.

In these enforcements, a number of Apps[10] were condemned publicly for their non-compliance, including their failure to publish rules on the collection and use of users' personal information, their failure to provide channels for users to access and revise their information, their failure to provide functions for users to cancel accounts, their unauthorized collection of personal information, their unreasonable requests for access, their unauthorized sharing of information with third parties, etc.

3. Key Regulatory Requirements

[6] https://tech.huanqiu.com/article/9CaKrnKkL7M
http://media.people.com.cn/n1/2019/0528/c40606-31105680.html

[7] http://www.miit.gov.cn/n1146295/n1652858/n1652930/n4509627/c7021505/content.html

[8] http://www.samr.gov.cn/xw/xwfbt/201911/t20191118_308613.html

[9] http://www.gov.cn/fuwu/2019-11/07/content_5449660.htm

[10] http://m.ccidcom.com/yaowen/20190705/NuighyttSvE1F7nXH16qaia44y0ts.html, http://www.xinhuanet.com/fortune/2019-12/19/c_1125365352.htm,http://miit.gov.cn/n1146290/n1146402/n1146440/c7619663/content.html

In accordance with the said regulations and the enforcement thereof, App operators need to focus particularly on the following requirements:

(1) An App shall instruct the user by pop-ups or other eye-catching displays, to read the privacy policy when the user runs the App for the first time, and shall not ask for the user's consent by assuming a default acceptance of the privacy policy if the user does not otherwise select or in any other implied manner;

(2) The purpose, method, scope and other details of the collection of personal information by the App (including any entrusted third party or any embedded third party code or plug-in) shall be specifically indicated in the App's privacy policy;

(3) When applying for a permit to enable access to personal information on a mobile phone, or applying for the collection of sensitive personal information, the App shall notify the user of their purpose simultaneously;

(4) The App shall not collect personal information, or change the 'allow or deny' status access to personal information set by the user, without the user's consent;

(5) When sending targeted pushes by using the user's personal information and algorithm, the App shall provide an option for the user to reject such targeted pushes;

(6) The App shall provide the user with the means or methods to withdraw their consent to personal information collection;

(7) The App shall provide functions for the user to deregister their account; and

(8) The App shall not force the user to permit the collection of any unnecessary information or enable any unnecessary access on a mobile phone.

4. Compliance Suggestions

In the said law enforcements, all the non-compliant App operators were warned or ordered to make corrections within a required time limit or be shut down or removed from App stores. Personal information protection has become an essential concern of App operators with respect to their compliance.

We suggest that any App operator who fails to conduct a self-examination, or to audit the entire process of the collection and usage of personal information, or fails to update their privacy policy, in accordance with the said regulations, should consider taking the following actions to ensure the compliance of their App on an ongoing basis:

(1) Confirm and check the entire process of data collection and use in the App, including the type, scope, scenario and reason for collection, and the method and scope of use;

(2) To carefully consider and check the necessity of sharing, contractual arrangement and liability assumption with respect to the sharing of personal information with third parties;

(3) To evaluate and justify relevant arrangement from various aspects such as collection, usage, duration of storage, and place of storage, etc. and

(4) To make corrections and update their privacy policies.

In addition to Apps, we also suggest updating and improving other online tools, including website and WeChat mini programs, by reference to the regulatory requirements on Apps.

We will keep our eye on any further requirements on the compliance of online tools.

Marissa Dong Partner Tel: 86 10 8519 1233 Email Address：dongx@junhe.com
Yuan Qiong Associate Tel: 86 10 8519 2410 Email Address：yuanq@junhe.com