



July 30, 2013

MIIT Issues Provisions Governing Protection of Personal Information of Telecommunications and Internet Users

Charles LI | Rae LIU | Arong

On July 16, 2013, the Ministry of Industry and Information Technology (“**MIIT**”) published the *Provisions for Protection of Personal Information of Telecommunications and Internet Users* (“**MIIT Provisions**”), to implement the *Decision to Strengthen Network Information Protection* (“**NPC Decision**”) issued by the Standing Committee of the National People’s Congress on December 28, 2012 and further Strengthen the protection of the personal information of telecommunications and internet users.

The MIIT Provisions have twenty five (25) clauses that specify: 1) the scope of protection and entities that bear protection obligations, 2) the specific obligations of telecommunications business operators and internet information service providers when collecting and using personal information from users, 3) agency management and supervision, 4) information security measures, 5) administrative supervision, and 6) penalties for violations. The key points of the MIIT Provisions are as follows.

1. Clarified Scope of Protected Personal Information and Entities Who Bear Protection Obligations

The NPC Decision broadly states that personal network information, meaning electronic information that identifies an individual and involves such individual’s privacy, shall be protected. Under the MIIT Provisions, the “personal information of telecommunications and internet users” to be protected is defined as information collected by telecommunications business operators or internet information service providers in the provision of services. Such personal information can individually or in combination with other information be used to distinguish a user, such as the name, date of birth, identification card number, address, telephone number, login username, login number, account, time and place.

Unlike the NPC Decision, which requires that “network service providers” shall bear the

obligations to protect personal network information, the MIIT Provisions identify the obligated entities as “telecommunications business operators or internet information service providers”.

2. Rules for Information Collection and Use

According to the principles set forth in NPC Decision, the MIIT Provisions require that the collection and use of personal information of telecommunications and internet users must be done on a legal, justified and necessary basis. Therefore, telecommunications business operators and internet information service providers are obligated under the MIIT Provisions:

- a. to formalize and publish their policies on information collection and use;
- b. not to collect or use personal information without consent from users;
- c. to notify users of the purpose, method, scope of data collection and other relevant matters;
- d. not to collect or use personal information when it's unnecessary;
- e. to stop information collection and use and to provide account cancellation services when telecommunications services are terminated;
- f. to refrain from any disclosure, distortion, damage, unlawful sale or provision of personal information to any third party;
- g. to establish and publish a compliant management process, and respond effectively within fifteen (15) days from receipt of any complaint.

3. Agency Management and Supervision

Pursuant to the principles the “one who conducts business shall be in charge” and the “one who delegates work shall be responsible”, as well as the agency theory in civil law, the MIIT Provisions require telecommunications business operators and internet information service providers to supervise and control agencies' activities when engaging an agency to provide end user services (such as marketing and technical services) to users and to collect and use the users' personal information. Additionally, any agency that fails to meet the requirements for personal information protection in providing any related service shall not be hired.

4. Detailed Information Security Measures

The MIIT Provisions set forth detailed information security protection measures to keep safe collected information from any leakage, damage, distortion or loss in areas such as roles and responsibilities, management system, authority, data storage mediums, information systems, operating records, and safeguards. The rules for information security incident handling and reporting, information protection self-inspection and training are also provided in the MIIT Provisions.

5. Administrative Supervision

The administrative authority related to network information protection is not specified in the NPC Decision. Under the MIIT Provisions, MIIT and its local counterparts are responsible for supervising the collection and use of the personal information of telecommunications and internet users, and may require the relevant telecommunications business operators or internet information service providers to submit related materials and access their premises to conduct inspections. MIIT and its local counterparts are required to examine the personal information protection rules during the annual inspection of telecommunications licenses. Any violation of the MIIT Provisions by telecommunications business operators or internet information service providers will be recorded in their social credit files.

6. Penalties for Violation

The NPC Decision generally provides that the legal liabilities for violating such decision include administrative penalties (warnings, fines, confiscating unlawful gains, revoking licenses or cancelling registration, closing down websites, etc.), criminal liabilities and/or civil liabilities. The MIIT Provisions further specify the administrative penalties for violating the relevant personal information protection rules that are set out in the MIIT Provisions below:

- a. Telecommunications business operators and internet information service providers who fail to formalize and publish policies on information collection and use, or establish and publish a compliant management process and respond effectively may be ordered to rectify within a specified period, and be subject to warnings and fines not exceeding RMB 10,000;
- b. Penalties for other violations in relation to information collection and use such as unlawful disclosure, distortion, damage, sale or provision of personal information to third parties, and failure to adopt regulatory information security measures, include rectification orders, warnings, fines ranging from RMB 10,000 to RMB 30,000, and public releases.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact **Charles Li (+86-10-8525 5518; charles.li@hankunlaw.com)**.