HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

February 26, 2013

NPC Standing Committee's Decision to Strengthen Network Information Protection

Jason WANG | Jialin ZHONG | Li YANG

On December 28, 2012, the Standing Committee of the 11th National People's Congress passed the *Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection* ("**Decision**") during its 30th session. The Decision has been in effect since the date of its promulgation. Prior to the release of the Decision, provisions relating to network information protection in China were scattered throughout various laws, administrative regulations, and administrative rules including but not limited to *Criminal Law*, *Tort Law*, and *Administrative Measures Governing Internet Information Services*.

The Decision has twelve (12) clauses that all regulate issues relating to network information protection such as the scope of protection, the entities to bear obligations and their specific obligations, the remedies to infringement, and the legal liabilities for violating the Decision. The key provisions of the Decision are as follows.

1. Specifies the Scope of Protected Network Information

The first paragraph of Clause I of the Decision states that "the State protects electronic information that identifies a citizen and involves a citizen's privacy." This provision specifies that "electronic information" that "identifies a citizen and involves a citizen's privacy" ("**Citizen's Personal Electronic Information**") is the type of network information protected by the Decision.

2. Prohibits Stealing, Illegally Acquiring, Selling, or Illegally Providing Citizens' Personal Electronic Information

The Decision explicitly prohibits any organization and/or individual from stealing, illegally acquiring, selling, or illegally providing to others Citizens' Personal Electronic Information.

This provision applies to "all/any organization(s) and/or individual(s)." While the Decision bans the act of illegally acquiring and/or providing Citizens' Personal Electronic Information, such information may be acquired or provided to others legally under certain situations (refer to Section 4 for more detail).

3. Prohibits Commercial Electronic Spam Information

The Decision also clearly prohibits any organization and/or individual from sending commercial electronic information to an individual's fixed line telephone, mobile phone, or e-mail box unless the electronic information recipient has agreed to or made a request to receive such information. This prohibition also applies if the recipient explicitly expresses his/her refusal. The primary purpose of this provision is to curb the flood of "audio advertisements," "short spam text messages," "spam email," and other kinds of commercial electronic spam information. This prohibitive provision also applies to "all/any organization(s) and/or individual(s)." Electronic information prohibited from being sent arbitrarily is limited to commercial electronic information.

4. Regulates the Collection, Utilization, and Preservation of Citizens' Personal Electronic Information in Business Activities

Besides those provisions that apply to all/any organization(s) and individual(s) as described above, the Decision also contains provisions that only apply to specific organizations and individuals. Network service providers as well as other enterprises and public institutions may need to collect, use, and preserve Citizens' Personal Electronic Information during business activities. The Decision acknowledges such needs, and provides certain rules they must follow to make such collection, utilization, and preservation more regulated. Specifically, they shall: (1) follow the principles of lawfulness, reasonableness, and necessity; (2) explicitly state the purpose, method, and scope of collection and/or use of the information; (3) obtain the consent of the those whose information is collected; (4) collect and/or use such information in accordance with the provisions of the relevant laws and regulations, and the agreement of the parties; and (5) make public their policies for collection and/or use.

The Decision requires network service providers as well as other enterprises and public institutions and their employees to keep strictly confidential Citizens' Personal Electronic information collected during their business activities, and prohibits them from disclosing, falsifying, damaging, selling, or illegally providing such information to others. Moreover, they shall also adopt technical and other necessary measures to ensure information security, and prevent the disclosure, damage, or loss of Citizens' Personal Electronic Information collected during their business activities. They shall immediately adopt remedial measures when information is or may be disclosed, damaged, or lost.

5. Specifies the Special Obligations of Network Service Providers

In addition to the above-mentioned obligations, network service providers[1] are subject to special obligations relating to network information protection, including:

1) Obligation to Manage the Information Released by Users

The Decision requires network service providers to strengthen their management of information released by their users. Once information prohibited from publication or transmission by laws or regulations is discovered, they shall immediately cease the transmission of such information, adopt measures such as removing and retaining relevant records and reporting to the relevant competent authorities. The *Administrative Measures Governing Internet Information Services* ("**Measures**") issued by the State Council in 2000 has a similar provision requiring all Internet information service[2] providers to manage information transmitted on their respective websites. The difference is that while the Measure requires Internet information service providers to assume this managerial obligation, the Decision imposes such obligation on all network service providers.

2) Obligation to Require Users to Provide Genuine Identification Information

The Decision also states that network service providers providing network access services, fixed-line telephone services, mobile phone services, or information posting services to users shall require the users to provide genuine identification information when signing a contract or when the provision of service is confirmed.

3) Obligation to Cooperate with and Provide Technical Support to Relevant Authorities

According to the Decision, when the relevant authorities perform duties in accordance with the law, network service providers shall cooperate with and provide technical support for them.

6. Specifies the Duties of Relevant Authorities for Network Information Protection

The Decision specifies that all relevant authorities shall carry out their duties within the scope of

[1] Under the current PRC laws and regulations, there is no clear and unified definition of the term "network service providers." As such, the discussion on the definition of the term still remains at the academic level. Some scholars think that the term "network service providers" refers to any institution that provides information to the public though an information network or provides the services necessary for obtaining network information. Such "network service providers" shall include individual users, Internet service providers, and non-profit organizations that provide facilities, information, or technical services such as intermediary and access services. Depending on the type of service provided, network service providers may be classified into network access service providers, network platform service providers, and network content and product providers.

See http://www.sipo.gov.cn/yl/2011/201102/t20110222_580220.html (last visited on February 22, 2013).

[2] According to the *Administrative Measures Governing Internet Information Services*, the term "Internet information services" is defined as "services providing information to online users through the Internet".

their functions and powers in accordance with law. They shall adopt technical and other necessary measures to prevent, stop, and investigate the criminal act of stealing, illegally acquiring, selling, or illegally providing Citizens' Personal Electronic Information, as well as any other network information-related criminal acts. However, the Decision does not specify the authorities related to network information protection. The particular authorities for network information protection are to be further clarified by more detailed rules/regulations regarding the Decision so that the relevant authorities may better perform their duties.

7. Specifies Infringement Remedies

According to the Decision, any citizen who discovers network information disclosing an individual's identity, distributing an individual's private information or otherwise infringing on his/her legitimate rights and interests, or whoever suffers harassment from commercial electronic information, has the right to require the network service provider to delete such information or take other measures necessary to stop the infringing act. By contacting network service providers directly and requiring them to stop the infringement, the infringed party may prevent more severe and extensive damages from occurring.

The Decision also provides that in the event of any network information-related illegal or criminal act[3] being discovered, both the party whose legal interests was infringed and any other third parties have the right to report or file a complaint with the relevant authorities and require such authorities to promptly handle any discovered illegal or criminal acts in accordance with the law.

The infringed party may also bring a lawsuit against the infringer according to the relevant laws and regulations. The infringer shall be held accountable for the civil liability of infringement.

8. Specifies the Legal Liabilities for Violating the Decision

According to the Decision, the legal liabilities for violating the Decision include:

1) Administrative liability. In the event of violating the Decision, administrative punishments that may be imposed include: warnings, fines, confiscating unlawful gains, revoking licenses or cancelling registrations, closing down websites, banning liable employees from engaging in network services business, and recording such employees in social credit files and making public thereof. Any act that constitutes a violation of public security administration shall be given public security administration punishments in accordance with the law.

[3] Such acts can include stealing, illegal acquiring, selling, or illegally providing to others Citizens' Personal Electronic Information.

2) Criminal liability. If such violation constitutes a crime, the offender shall be investigated for criminal liability accordingly.

3) Civil liability. In case of any act violating the Decision infringes on a citizen's civil rights and interests, the offender shall be subject to civil liability in accordance with the law.

It should be noted that the Decision only provides abstract principles on the legal liabilities for violating the Decision. Specific regulation is to be further clarified by the forthcoming detailed regulations/rules. The assumptions of legal liability shall also be determined according to other relevant criminal, administrative, and civil laws and regulations. We will continue keep an eye out for any future developments in the regulations/rules regarding Network Information Protection.

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 **Jason Wang** (**+86-755-3680 6518; jason.wang@hankunlaw.com**).