The 2014 GSR Policies and Regulatory Measures

Contribution from Ministry of Industry and Information Technology (MIIT), the People's Republic of China

I. China's Protection Measures and Related Practice

1. Service quality assurance

In recent years, in accordance with relevant laws and regulations, the Ministry of Industry and Information Technology (MIIT) of China has taken a series of measures to ensure the service quality：

1）In order to continuously benefit people's livelihood, MIIT mainly focuses on the implementation of "Broadband China" strategy by supervising and guiding broadband service providers to further improve the performance of their broadband networks and strengthening the monitor of broadband speed.

2) MIIT regularly carries out assessment of telecommunications service quality and also analysis of user complaint files, as well as takes specialized supervision for typical problems.

3) MIIT continually develops and reviews service quality standards and specifications of new technologies and services.

4) MIIT regularly organizes inspection on service specifications and charges by dialing to try relevant services, and in particular, addresses the problems which users mostly complain about, such as arbitrary charges of handset built-in services, VAS induced consumption, and unstable broadband service quality. Normally, the violators are strictly punished.

2. Security protection of user personal data

The Chinese government always keeps focusing on protecting the legitimate rights and interests of telecom/ICT users. The related work in recent years is mainly represented in the following aspects.

Firstly, China has begun to establish the legal system for protecting personal network information security. Currently , China has established and published a series of laws, regulations and standards, such as “Decisions on Strengthening the Protection of Network Information”, “Several Provisions on Regulating the Market Order of Internet Information Service”. Additionally, “Regulations on the Protection of Telecommunication and Internet Users’ Personal Information” has been issued in July, 2013. Also, there are some legislative trials and efforts on special protection in a couple of provinces in China.

Secondly, China has begun to build a management system for the administrative protection of personal network information. “Regulations on the Protection of Telecommunication and Internet Users’

Personal Information" has clearly defined the functional roles of the Telecom Regulatory Authority of MIIT (TRA) and the Communications Security Bureau of MIIT (CSB) on the security protection of personal network information. Specifically, TRA is responsible for the administrative affairs related to specifications on information collection and usage, and CSB take charge of the administrative affairs on security measures. Under the new framework, administrative investigations, warnings, punishments and other practical mechanisms for the security protection of personal network information are gradually put into force.

Thirdly, China has begun to establish a technical protection system for personal network information. General protection technologies for the security protection of personal network information such as attack and intrusion prevention are being applied, while special protection technologies such as anonymity and data protection models are under development. In recent years, China has begun to emphasize the related standards on security protection of personal network information and to develop such standards from the industrial and enterprise prospective. To prevent unauthorized access to the enterprise intranet and service system, China has built such technology platforms as centralized management and control and unified authentication at the enterprise level. In addition, MIIT has organized related entities to study and draft the "Requirements on the General Technology and Management of Protecting Network User

Information", and "Testing requirements on the Protection of Network User Information", which further specify the protection scope of personal information of telecommunications and Internet users, set targeted management and technology requirements on protecting users' personal information, as well as clarify the testing methods, processes and criterions. Moreover, the third-party certification service of security protection on personal information has started launching and exploring. Dalian Software Industry Association has created and implemented the "Evaluation and Certification Mechanism of Personal information Protection (PIPA Certification)", with reference to a number of local sectoral standards, for example, "Standards of Personal Information Protection in Dalian Software and Information Service Industry", "Standards of Personal Information Protection in Liaoning Software and Information Service Industry", and "Standards of Personal Information Protection in Liaoning Province (DB21/T1628-2008)". Based on national standards, China Software Testing Center has built and run the certification mechanism for the management system of personal information protection, to provide an overall evaluation of enterprise-class personal data protection.

Fourthly, China has begun to establish a self-regulatory system in the security protection industry of personal network information. In 2002, protecting network privacy was mentioned in the "China Internet Sector

Self-Discipline Convention" issued by the Internet Association of China. Furthermore, "Guidance on Personal Information Protection in the Public and Commercial Service Information System of Information Security Technologies", drafted by the China Software Testing Center associated with more than 30 entities, has been published as national standards and put into force on February 1, 2013.

3. Security protection for smart terminal users

The MIIT, as the governing body of telecom/ICT industry, has strengthened the administration on network entry licensing of smart mobile terminals, and regulated the market in accordance with related laws and regulations such as "Standing Committee of the National People's Congress Decisions on Strengthening the Protection of Network Information" and "Telecommunications Regulations" since 2013.

1) MIIT has issued sectoral standards and increased the intensity on examining pre-installed software in smart terminals.

2) MIIT has strengthened the spot check on smart terminals to urge enterprises to strictly comply with relevant standards and imposed penalties for non-compliance.

3) MIIT has also raised the efforts on governing mobile Internet malwares. According to the "Monitoring and Response Mechanism for Mobile Internet Malwares" published in 2011 by MIIT, governance has been undertaken to fight mobile Internet malwares relevant to malicious

fee deduction, resources consumption, system damage and privacy theft for ensuring the security of connected smart terminals.

II. Proposals from China

Currently, the new technologies and services with Internet as the core have seriously challenged the scope, boundary, essence, content of telecom/ICT users' traditional rights and obligations. Following the technology trends, the important issue for governments and international organizations to address is to establish and improve the security assurance system in terms of the consumption and application levels for constantly providing confidence and motivation to technology development. Consequently, we propose:

1. Considering the actual protection demands of users' rights and interests from multiple perspectives

Through the relative policy practice and internationally bilateral or multilateral consultations，it is likely to make a more comprehensive list of legitimate consumer rights and interests, which include equal and universal access, right to know and select, peaceful right, right to express, privacy right, personal data right, intellectual property right and virtual property right, etc., and can be universally and equally protected within the scope of laws and regulations.

2. Defining priorities and responsibilities of regulatory authorities in the digital environment

1) facilitating the deployment of the next generation network

It is advised to coordinate the network construction, analyze the universal broadband service regime and constantly narrow the coverage gap among regions and between urban and rural areas. Additionally, it is necessary to drive the commercial development of 4G , organize researches on 5G, promote the rational distribution of such application infrastructures as IDC and CDN, and guide the evolvement of supporting networks and websites to IPv6.

2) fostering and expanding the consumption of information service

It is suggested to: a) guide basic telecom operators to lower the network service price for triggering the dynamic of market demand and promoting the wide application of network technologies; b) implement a number of pilot projects of mobile internet, cloud computing, big data and internet of things in key industries and fields; c) coordinate related enterprises to strengthen the financial support for the research and commercialization of core technologies; d) innovate policies to promote the development of convergence services, such as IPTV, mobile TV, and Internet TV.

3) Adjusting policies for the protection of personal data rights

With reference to the development of new technologies and new services, such as big data, cloud computing, social networks and mobile Internet, it is necessary to modify the description of various rights in terms of the inherent boundary, category, derivative rights, licensing format and usage pattern by overall considering the concept, scope, type, legitimate collection and usage, security protection principles of privacy rights and personal data rights.

Firstly, an integral ecosystem of personal data rights needs to be established. The ecosystem can be composed of the derivate rights of privacy rights and personal data rights including the right to delete, to forget and to carry, as well as the right to permit, to select, to access, to know, to secure, to correct, to oppose, and to seal.

Secondly, it is necessary to consider the redefinition of personal data. All individual-related personal information which can provide direct or indirect clues and associated assistance to identify an individual, may be personal data and be equally protected by the law, instead of classifying personal information as identity-based information and non-identity-based information.

Thirdly, an updated licensing trust model of personal data collection needs to be established. It is necessary to consider the possibility of revising and improving the licensing model of personal information with

a view to rebuild the licensing trust model between data processors and data owners by the massive application of presumed consent and massive licensing, while one-to-one licensing as the special case.

3. Expanding the regulator’s mandate and enforcement measures

To adapt to the continuous development of new technologies and new services, it is required to reconsider the mandate of telecom/ICT regulators with a view to strategically transfer the enforcement priority from traditional administrative areas to the new ICT governance associated with market behavior, market competition, data protection and security conformance.

1) to authorize the telecom/ICT regulators to protect the legitimate rights and interests of users. Internationally multilateral elaboration and rule-making may be used to drive the establishment of an international coordination mechanism for protecting legitimate rights and interests of telecom/ICT users , and the domestic protection agencies at multiple levels need to be promoted as well.

2) to authorize telecom/ICT regulators to take integral enforcement in accordance with the law. Specifically, it may consider the introduction of administrative examination and approval, registration and declaration system regarding to the collection and process of personal information for improving the enforcement system of administrative protection, as well as

the introduction of administrative assessment, investigation, public hearing, mandatory statement, cease-and-desist, injunction, punishment, and other measures to enhance the enforcement measures of administrative protection.3) to authorize the telecom/ICT regulators to protect the cyber security. A series of policy measures can be prioritized to establish self-adaptive, self-correcting and self-healing virtual social relationships for spam, undesirable content, network misconduct and for virtual property, information resources, network contract and network media , and then build a secure and reliable cyber space covering terminals, information sources, application and content, equipment, networking and infrastructures.