君合研究简讯

JUNHE

2016年1月8日

信息保护和网络安全热点问题

《反恐怖主义法》对电信及互联网行业的影响

第十二届全国人大常委会第十八次会议于2015年12月27日由正式通过了经过三次审议的《中华人民共和国反恐怖主义法》（以下简称“**《反恐法》**”），该法将于2016年1月1日起施行。《反恐法》是中国打击恐怖主义方面的首部专项法律，其规定内容十分广泛，涵盖了反恐怖主义工作的各个方面。《反恐法》规定电信和互联网企业在政府有关部门防范和调查恐怖主义活动中的协助义务，此规定可能在一定程度影响未来互联网和科技公司在中国的运营。

一、《反恐法》关于电信和互联网行业的规定

1、技术接口和解密协助

根据《反恐法》，电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法防范和调查恐怖主义活动的工作提供技术接口和解密等技术支持和协助。然而，《反恐法》并未进一步明确规定相关政府机构要求提供协助所需履行的程序及文件。

2、防止恐怖主义信息传播

《反恐法》还规定，电信业务经营者、互联网服务提供者应当依照法律、行政法规规定，落实网络安全、信息内容监督制度和安全技术防范措施，防止含有恐怖主义、极端主义内容的信息传播；发现含有恐怖主义、极端主义内容的信息后，应当立即停止传输，保存相关记录，删除相关信息，并向公安机关或者有关部门报告。

3、身份验证义务

此外，《反恐法》还明确规定电信与互联网企业当履行身份验证义务。根据《反恐法》，电信业务经营者、互联网服务提供者应当对客户身份进行查验，对身份不明或者拒绝进行身份查验的客户不得提供服务。然而，《反恐法》并未进一步明确规定电信业务经营者、互联网服务提供者应当采取的具体验证措施。内容监督和实名制要求已体现在许多现有法规中，而《反恐法》将此类对电信和互联网经营者的要求上升到法律高度，并扩大适用至所有类别的电信和互联网服务。

4、法律责任

根据《反恐法》，违反上述规定的电信和互联网业务经营者可能被处罚款，其直接负责的主管人员和其他直接责任人员则可能被处罚款或拘留。

二、与《反恐法（草案）》的简要对比

与全国人民代表大会常务委员会于2014年11月公布征求意见的《中华人民共和国反恐怖主义法（草案）》相比，《反恐法》终稿删除了一些有争议的条款，例如电信业务经营者、互联网服务提供者应当在电信和互联网的设计、建设和运行中预设技术接口，将密码方案报密码主管部门审查，以及将相关设备、境内用户数据留存在中华人民共和国境

内等。

三、法律点评

总体而言，《反恐法》中规定的义务仍存在模糊不清之处，给有关部门解释和执行该法留下较大空间。例如，《反恐法》并未明确界定承担上述协助义务的电信和互联网经营者的具体范围。相关部门可能在未来颁布更具体的执行细则来进一步明确相关义务。我们建议电信和互联网企业密切关注此领域的发展动向。

董　潇　　合伙人　　电话：86 010 8519 1233　　邮箱地址：dongx@junhe.com
蔡克蒙　　律　师　　电话：86 010 8519 1255　　邮箱地址：caikm@junhe.com

JUN HE BULLETIN

JUNHE

January 8, 2016

Information Protection and Cyber Security

The Counter-Terrorism Law and Its Implication to Telecom and Internet Companies

After three deliberations, the *Counter-Terrorism Law of the PRC* ("**CTL**") was formally promulgated by the National People's Congress Standing Committee ("**NPC Standing Committee**") on December 27, 2015, and took effect from January 1, 2016. The CTL is the first counter-terrorism law in China, which includes wide-ranging stipulations and is intended to cover to all aspects of counter-terrorism activities. Among other things, the CTL provides obligations for telecom and Internet enterprises to cooperate with government authorities in investigating terrorism activities, which may have a significant impact on the operation of Internet and tech firms in China.

Technical Interfaces and Decryption Assistance

According to the CTL, telecom and Internet service providers are required to provide technical interfaces and technical assistance in decryption and other efforts to public and national security authorities engaged in the lawful conduct of terrorism prevention and investigation. However, the CTL does not further specify the procedure and documentation required for the authorities to make such requests for assistance.

Preventing the Dissemination of Terrorism Information

The CTL also requires Internet service providers to implement network security and information and content monitoring systems and adopt technical security measures to prevent the dissemination of information containing terrorist or extremist content. Once such content is detected, Internet service providers shall cease the transmission of the information, keep the relevant records, delete the information and report the occurrence to public and national security bodies.

Identity Verification Requirements

In addition, the CTL clearly stipulates the real-name requirement for telecom and Internet providers. Under the CTL, telecom and Internet providers are required to verify the identity of their clients, and to not provide services to anyone whose identity is unclear or who declines to verify

his/her identity. However, the CTL does not further specify the required measures for verification by telecom and Internet providers. Although the content monitoring and real-name requirements are already embodied in various regulations, the CTL extends these requirements to all types of telecom and Internet services as statutory obligations of the service providers.

Legal Liability

According to the CTL, telecom and Internet providers violating the aforesaid requirements may be subject to fines and their direct responsible persons may be subject to personal liabilities of fines and detention.

Brief Comparison with the Draft Released for Public Comment

Compared with the earlier draft of the CTL released by the NPC Standing Committee in November 2014 for public comment, the final CTL leaves out controversial language requiring telecom and Internet service providers to file their encryption plans with the encryption authority for review; pre-install interfaces in the design, construction and operation of telecommunication and Internet programs; and store their device and users' data within the PRC.

Our Observation

In general, the obligations embodied in the CTL are still vague and ambiguous, and the CTL leaves large room for the authorities in terms of interpretation and implementation. For example, the CTL has not even provided a clear scope of telecom and Internet service providers subject to these requirements. The relevant government authorities may promulgate further implementing rules to stipulate the obligations. We suggest that telecom and Internet companies closely follow the developments in this area.

Marissa (Xiao) DONG	Partner	Tel：86 10 8519 1233	Email：dongx@junhe.com
Clement (Kemeng) CAI	Associate	Tel：86 10 8519 1255	Email：caikm@junhe.com