Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 31 • NUMBER 10 • OCTOBER 2019

CAC Releases Regulation on the Protection of Children's Personal Information Online

Yan Luo, Zhijing Yu, and Nicholas Shepherd

The Cyberspace Administration of China (CAC) released the *Regulation on the Protection of Children's Personal Information Online* (Regulation) on August 23, 2019.[1] It went into effect on October 1, 2019.

Earlier this year, CAC issued the draft *Measures for Data Security Management* (Draft Measures), which set out the general regulatory framework that will govern the collection and use of personal information by network operators (broadly defined as "owners and managers of networks, as well as network service providers"). The release of this new Regulation demonstrates CAC's intention to set out more stringent requirements for network operators if they collect, store, use, transfer, or disclose the personal information of minors under 14 years old. This article discusses the key requirements of the Regulation in greater detail.

Yan Luo is of counsel at Covington & Burling LLP advising clients in an array of regulatory matters in connection with international trade, cybersecurity, and antitrust/competition laws. **Zhijing Yu** is an international associate at the firm advising multinationals and Chinese companies on an array of matters in connection with data privacy, cybersecurity, international trade, and corporate transactions. **Nicholas Shepherd** is an associate at the firm, where he is a member of the Data Privacy and Cybersecurity practice group, advising clients on national and international issues related to data protection and information security. The authors may be contacted at yluo@cov.com, zyu@cov.com, and nshepherd@cov.com, respectively.

Notice and Consent

The Regulation requires network operators to adapt their policies and agreements, as well as internal procedures, for handling children's personal information.[2] Also, guardians must be notified in a prominent and clear manner of the collection and use of children's personal information and network operators must obtain consent from guardians for such collection and use.[3]

Similar to the requirements specified in the Draft Measures, the Regulation requires that privacy notices to guardians include the following information:

- the purposes, scope and methods for the collection, storage, use and disclosure of children's personal information, as well as the retention period;
- location of data storage and what the network operator will do with the children's personal information after the retention period expires (e.g., delete or anonymize);
- security measures adopted to protect children's personal information;
- the consequence(s) for refusing to provide consent;

- the channels and means by which to file a complaint; and

- the means available to correct and delete children's personal information.

If there are any substantial changes to the information provided in the privacy notice, then network operators are required to obtain consent from guardians for those changes.[4]

Responsible Person for Children's Personal Information Protection

The Regulation requires network operators who collect and use children's personal information to designate a person responsible for the protection of children's personal information.[5] It is unclear whether this requirement also applies to companies that collect children's personal information during their general business operations, but do not specifically target children, although in general the Regulation does not make this distinction.

Internal Access Controls

The Regulation requires network operators to establish internal access controls to protect children's information. The access to children's personal data by employees must be authorized and recorded by the responsible person for children's personal information protection. Network operators are also required to adopt technical measures to prevent employees from illegally copying or downloading children's personal information.[6]

The Regulation requires network operators to establish internal access controls to protect children's information.

Third-Party Processors

When third-party vendors are engaged to process children's personal information, network operators are required to conduct a security assessment and specify security obligations and requirements in agreements with these vendors. It is uncertain whether this assessment has to be conducted before engaging a vendor.

The Regulation also imposes specific obligations on vendors, requiring them:[7]

- To process children's personal information according to the instructions of network operators;

- To provide assistance to network operators in responding to requests made by guardians of children;

- To adopt measures to protect children's personal information and timely report the occurrence of any data breaches to network operators;

- To timely delete children's personal information when the processing agreement is terminated; and

- Not to engage any sub-processors to process children's personal information.

Furthermore, network operators are prohibited from publicly disclosing children's personal information unless required by law or agreed to by guardians.[8]

Rights to Children's Personal Information

Children and/or their guardians have the right to require network operators to correct children's personal information that is inaccurate,[9] as well as to require the deletion of children's personal information[10] if:

- The network operator collects, stores, uses, transfers or disclose children's personal information in violation of laws, regulations or user agreements;

- The network operator collects, stores, uses, transfers or disclose children's personal information for unnecessary purposes or for a period beyond the necessary retention period;

- A guardian withdraws consent; or,

- A child or its guardian indicates that it no longer uses the respective products or services (e.g., by closing an account or other similar actions).

These rights are largely consistent with general personal information rights found in China's national standard for personal information protection (hereafter the Standard) for example, both

have a straightforward "account cancellation" right. However, the Regulation is less prescriptive in certain aspects. For example, while the Standard requires that rights requests be complied with in less than 30 days (or other legally stipulated period), the Draft Regulation only requires their fulfillment "in a timely manner."

Network operators are required to carry out their emergency response plan and adopt remedial measures when a data breach occurs (or is suspected to have occurred).

Automated Data Processing

Under the Regulation, if an automated processing system cannot identify whether the data processed is children's personal information or not, then such processing must still comply with "other relevant rules" as applicable.[11] It is currently unclear what "other relevant rules" would apply in this scenario.

Incident Response

Network operators are required to carry out their emergency response plan and adopt remedial measures when a data breach occurs (or is suspected to have occurred). Additionally, if the data breach results in (or may result in) "serious consequences" (a term which is not defined in the Regulation), then network operators must report this to regulators and notify affected children and their guardians. If individual notification presents an undue burden to network operators, an announcement shall be issued in a reasonable and effective manner.[12] Again, this requirement is consistent with the breach notification requirements in the Standard, which require "network operators" to notify an incident to regulators and affected individuals when there has been actual or potential "leakage, damage, or loss" of personal data.

Potential Penalties

CAC may "summon" a network operator to discuss the issues with them, if (i) it fails to comply with its data protection obligations; or (ii) its handling of children's personal information presents high security risks; or (iii) a data breach occurs. After meeting with CAC, the network operator may be ordered to rectify its conduct.[13] The CAC or other agencies may also impose a fine or other penalties for violations of the Regulation in accordance with China's Cybersecurity Law or Administrative Measures for Internet Information Services. If the violation constitutes a crime, the network operator may be subject to criminal prosecution.[14]

Notes

1. The official Chinese version of the Regulation is available at *http://www.cac.gov.cn/2019-05/31/c_1124568048.htm*.
2. Article 8.
3. Article 9.
4. Article 10.
5. Article 8.
6. Article 15.
7. Article 16.
8. Article 18.
9. Article 19.
10. Article 20.
11. Article 28.
12. Article 21.
13. Article 25.
14. Article 26.