# PRC Data Security Updates (2021)

谢融/Rong Xie
吕冠贤/Dominic Lui
上海融浩知识产权顾问有限公司/Fuxion IP Consulting, Co. Ltd.

# 免责声明/DISCLAIMER

此处所提供的信息和资料不是、也不应被视为法律建议。此处信息和资料没有用于建立律师与客户关系的目的。如有法律问题，最好的解决办法是寻求拥有专业知识的人士咨询有效建议。该展示资料不应被依赖用于、或代替与专业人士的咨询。

The information presented here is not and should not be considered as legal advice. The information here is not intended to create a lawyer-client relationship. When confronted with legal issues, it is always the best practice to find someone who has the expertise necessary to provide meaningful advice. Information from this presentation should not be relied upon or used as a substitute for consultation with professional advisors.

# Overview

1. *The "Didi" incident and Cybersecurity Law of 2017*
2. *Data Security Law of 2021*
3. *Regulation of Human Genetic Resources of 2019*

# The "Didi" Incident

1. July 2, 2021 China's Cybersecurity Review Office ("CRO"), an office established under the Cyberspace Administration of China ("CAC") announced that it had initiated a cybersecurity review against Didi Chuxing ("Didi").

2. The Didi app was subsequently removed from app stores.

3. Legal authority of the review:
   - The National Security Law ("NSL")
   - the Cybersecurity Law ("CSL"); and
   - the Measures on Cybersecurity Review ("Measures").

4. Purpose of the review:
   - "preventing national data security risks, maintaining national security and safeguarding public interests."

# The CSL Requirements

1. Effect on June 1, 2017, aiming at protecting key information infrastructure and considers Critical Information Infrastructure ("CII") critical for safeguarding China's national security.

2. Requires CII Operators to undergo a security review if the procurement of "network products and services" implicates China's national security.

    1) "Network products and services" cover:
        - "core network equipment, high-capability computers and servers, high-capacity data storage, large databases and applications, network security equipment, cloud computing services," and other network products or services that have an important impact on CII.

3. Imposes restrictions on the transfer of personal information and business data overseas. Penalties include suspension of business activities, close of businesses, revocation of licenses, and a fine of up to RMB1,000,000.

# The Interagency Review

1. A high-level interagency review body with members from 11 agencies ("Members"), including CAC, the Ministry of Industry and Information Technology ("MIIT"), the Ministry of Public Security, the Ministry of National Security, and the State Administration for Market Regulation.

2. Regular review process - CRO and Members will complete the review and issue a written notification to the CII Operator within 45 working days (extendable by 15 business days, pending complexity)

3. Special review process - If no consensus can be reached in the regular review process, CRO and Members will take another 45 working days (extendable pending review complexity) to complete the process.

4. Root Cause of the Didi incident?
   "in the listing process in the US, some important data and personal information held by Chinese companies may be revealed due to the US regulation request" and thus "(public) listing in the US could lead to security risks."

5. Current review may focus on "risks associated with cross-border transfer of important data and personal information."

# The DSL

1. On June 10, 2021, the Standing Committee of China's National People's Congress ("NPC") enacted the Data Security Law ("DSL"), which will take effect on September 1, 2021.

2. The DSL aims to regulate a wide range of issues in relation to the collection, storage, processing, use, provision, transaction and publication of any kind of data, and shall become a key supplement to the CSL.

3. Highlights of DSL include:

    1) Request for data by judicial and enforcement agencies outside of China.
    2) Systems to protect in-country Data
    3) National security review of certain data processing activities
    4) Chinese government access to data.

# Data transfer to judicial and enforcement agencies outside China

1. The DSL prohibits "provid[ing] data stored within the PRC to foreign judicial or law enforcement bodies without the approval of the competent authority of the People's Republic of China."

2. Applicable to the transfer of any data, regardless of subject matter and sensitivity, so long as it is stored in China (Article 36).

3. Companies failing to obtain a prior approval may be penalized:
   1) a fine of up to RMB 1,000,000 and fines for responsible individuals; or
   2) a fine of up to RMB 5,000,000, suspension of business operations, revocation of business licenses, as well as increased fines for responsible individuals

4. Privacy shields under other jurisdictions shall be tested in a context of cross-boarder investigation or litigation.

# Systems to protect in-country Data

1. The DSL generally requires entities and individuals operating within China to implement systems designed to protect in-country data.

    1. Entities that handle "important" data must designate personnel responsible for data security and conduct assessments to monitor potential risks.

        - Failing to satisfy these requirement:
            - ❖ a fine of up to RMB 500,000 and mandatory remedial actions; or
            - ❖ after receiving a warning and/or a large-scale data breach - a fine of up to RMB 2,000,000, revocation of business license and fines to responsible individuals.

    2. "Core Data" include "data related to national security, national economy, people's welfare, and major public interests."

        - "Violation of the national core data management system or endangering China's national sovereignty, security, and development interests":
            - ❖ a fine up to RMB 10 million, suspension of business, revocation of business licenses, and in severe cases, even criminal liability.

# National security review and Government access to data

1. The DSL calls for the establishment of a system for “national security review” to examine any data activities that may pose risks to national security (Article 24).
2. The decision of the national security review is final and non-appealable (Article 24).
3. China’s public security bureaus and national security agencies can request data for national security and criminal investigations, as long as proper procedures are followed (Article 35).
4. Individuals and organizations are obligated to comply with such requests (Article 35).

# Overview: Regulations of Human Genetic Resources

1. The Interim Measures for the Administration of Human Genetic Resources has been in force since 1998, but has several limitations: lack of specific legal liabilities, insufficient regulatory measures and standardization

2. Since July 1, 2019, the Regulation on the Administration of Human Genetic Resources has taken effect in China.

3. The Regulation aims to regulate issues in relation to handling of human generic resources (HGR), including collecting, preserving, using and providing HGRs to foreign parties

4. Definition of human generic resources (HGR): HGR **materials** and HGR **information**
    1. HGR information: **Data** and other information produced from HGR materials

5. Key highlights for local parties:
    1. Buying and selling of HGRs prohibited (Article 10)
    2. Requirements for collecting and preserving HGRs – ethical review (Article 11, 14)
    3. Ministry of Science and Technology (MOST) has the power to perform on-site inspections, review and copy materials, or seize HGRs (Article 34)

# Involvement of Foreign Parties

1. Prohibitions
   1. Foreign parties must NOT collect or preserve HGRs in China
   2. Foreign parties must NOT provide China's HGRs outside of China (Article 7)

2. Approval required
   1. International collaboration for research (Article 19, 22)
   2. Transferring HGR **materials** to foreign parties during collaboration with foreign (Article 27)

3. Notification (to MOST) required
   1. International collaboration for clinical trials (Article 22) which do not involve HGR materials crossing the borders
   2. Transferring HGR **information** to foreign parties or open for public use, but must **notify** MOST (Article 28)

# Penalties

1. Large penalties for breach of regulations:
    1. Companies collecting and preserving HGRs without permission: RMB 500,000 to 5,000,000 for unlawful gains below RMB 1,000,000; 5x to 10x of such gains for unlawful gains over RMB 1,000,000 (Article 36)
    2. Foreign parties collecting/preserving/providing across borders HGRs: RMB 1,000,000 to 10,000,000 for unlawful gains below RMB 1,000,000; 5x to 10x of such gains for unlawful gains over RMB 1,000,000 (Article 41)
    3. Serious violations: Prohibition from engaging in activities relating to HGRs for 1-5 years, permanently for especially serious cases (Article 43)

# Case Study

Note: Cases presented are on the basis of the Interim Measures of 1998.

1. BGI, Huashan Hospital and Oxford University (2015):
   1. International collaboration for research + HGR information published online without approval
   2. Punishment: Stop and destroy all HGR materials and information from such research, suspend international collaboration

2. WuXi AppTec (Suzhou) (2016):
   1. Human serum was transferred across borders as canine blood plasma
   2. Punishment: Warning, destroy all HGR materials related to project, suspend accepting applications from company for international collaboration

# Case Study – Continued

3. AstraZeneca, Amoy Diagnostics, $Q^2$ Solutions (2018):
   1. Activities exceeded the approved scope of international collaboration for research (leftover samples from research transferred to other companies)
   2. Punishment: Warning, destroy all HGR materials related to project, revocation of licenses, suspend accepting applications from company for international collaboration

4. Icon Clinical Research, Bristol Myers Squibb (2020):
   1. Forged seals/signatures, false information submitted in application materials for international collaboration
   2. Punishment: Suspend accepting applications from company for international collaboration

Takeaways:

- Large companies certainly NOT immune from the Regulations
- Punishment were relatively lenient based on Interim Measures of 1998. Future violations may be subject to harsher punishment on the basis of the Regulations of 2019.

# Questions?

问题？

# THANK YOU!

## 感谢您的参与!

# Contact Us

Please follow us on

WeChat:

融浩知产FUXION IP

Rong Xie:

rx69764


- Contact: Rong Xie
- Phone: +86-13816732189 (PRC); +1-6463213080 (U.S.)
- Email: rongxielaw@163.com
- WeChat: rx69764