Unofficial English Translation by Morgan Lewis

Original Source

The Relevant Person-In-Charge of the Cyberspace Administration of China (CAC) Answers Media Questions Regarding the Administrative Penalty decision Lawfully Made Against DiDi Global Co., Ltd Related to the Cybersecurity Review

July 21, 2022

On July 21, the CAC announced the decision to impose administrative penalties related to cybersecurity review on Didi Global Co., Ltd. (hereinafter referred to as "Didi ") in accordance with the law. The relevant person in charge of the CAC answered reporters' questions about the case.

1. Q: Please briefly introduce the background and investigation process of the case?

A: In July 2021, in order to prevent national data security risks, safeguard national security and protect public interests, according to the National Security law and the Cybersecurity Law, the Cybersecurity Review Office implemented cybersecurity review on Didi in accordance with the cybersecurity review measures.

According to the conclusion of the cybersecurity review and the problems and clues found, the CAC filed a case for investigation of the suspected illegal acts of Didi according to law. During this period, the CAC conducted investigations and technical evidence collection, ordered Didi to submit relevant evidence materials, conducted in-depth verification and analysis of the evidence materials of this case, fully listened to the opinions of Didi, and guaranteed the legal rights of Didi. It is verified that Didi's violations of the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law have clear facts, conclusive evidence, serious circumstances, and vile nature, and should be severely punished.

2. Q: What are the illegal behaviors of Didi?

A: After investigation, there are 16 illegal facts in Didi, which can be summarized into 8 aspects. First, illegal collection of 11.9639 million screenshots in users' mobile photo albums; second, over collecting 8.323 billion pieces of user clipboard information and application list information; thirdly, 107 million pieces of passenger face recognition information, 53.5092 million pieces of age information, 16.3356 million pieces of career information, 1.3829 million pieces of family relationship information, and 153 million pieces of taxi address information of "home" and "company" were excessively collected; fourth, 167 million pieces of accurate location (longitude and latitude) information were collected when passengers evaluated valet service, APP background operation, and mobile phone connected to orange recorder equipment; fifth, 142,900 pieces of driver's academic information were excessively collected, and 57.8026 million pieces of driver's ID number information were stored in clear text; sixth, analyze 53.976 billion pieces of passenger travel intention information, 1.538 billion pieces of resident city information, and 304 million pieces of non-local business/non local tourism information without clearly informing passengers; seventh, passengers frequently asked for irrelevant "phone permission" when using the free ride service; eighth, 19 personal information processing purposes such as user equipment information were not accurately and clearly explained.

Previously, the cybersecurity review also found that Didi had data processing activities that seriously affected national security, as well as other violations of laws and regulations such as refusing to comply with the explicit requirements of the regulatory authorities, openly obeying but secretly violating, and maliciously evading supervision. Didi's illegal operations have brought serious security risks to the security of national critical information infrastructure and data security. Because it involves national security, it is not made public according to law.

3. Q: How to identify the illegal subject of this case?

A: Didi was founded in January 2013. The relevant domestic business lines mainly include online car hailing, free ride, two-wheeler, car making, etc. the relevant products include 41 apps, including Didi travel app, Didi owner app, Didi free ride app, Didi enterprise app, etc.

Didi has the highest decision-making power on major issues of domestic business lines, and the internal system and norms formulated by the company are applicable to all domestic business lines, and it is responsible for the supervision and management of the implementation. Through Didi information and data security committee and its subordinate personal information protection committee and data security committee, the company participated in the decision-making guidance, supervision and management of online car hailing, hitchhiking and other business line related behaviors. The illegal behaviors of each business line were specifically implemented under the unified decision-making and deployment of the company. Accordingly, the subject of the illegal act in this case is identified as Didi.

Cheng Wei, chairman and CEO of Didi, and Liu Qing, president, are responsible for violations.

4. Q: What is the main basis for the decision to impose administrative penalties related to cybersecurity review on Didi?

A: The administrative penalties related to the cybersecurity review of Didi is different from the general administrative punishment and has particularity. Didi's violations of laws and regulations are serious and should be severely punished in combination with the cybersecurity review. First, from the nature of the illegal act, Didi failed to perform its obligations of cybersecurity, data security and personal information protection in accordance with relevant laws and regulations and the requirements of the regulatory authorities, ignoring the national cybersecurity and data security, bringing serious risks to the national cybersecurity and data security, and when the regulatory authorities ordered it to correct, comprehensive and in-depth rectification has not been carried out yet, and the nature is extremely vile. Second, from the perspective of the duration of the illegal acts, the relevant illegal acts of Didi began in June 2015 and have lasted for up to seven years. They have continued to violate the Cybersecurity Law implemented in June 2017, the Data Security Law implemented in September 2021 and the PIPL implemented in November 2021. Third, from the perspective of the harm of illegal acts, Didi collects personal information such as user clipboard information, screenshots in photo albums and family relationship information through illegal means, which seriously infringes on users' privacy and their personal information rights and interests. Fourth, in terms of the number of illegal processing of personal information, Didi illegally processed 64.709 billion pieces of personal information, a huge number, including face recognition information, accurate location information, ID number and other sensitive personal information. Fifthly, from the perspective of illegal processing of personal information, Didi's illegal activities involve multiple apps, including excessive collection of personal information, compulsory collection of sensitive personal information, frequent claims on apps, failure to fulfill the obligation of informing about personal information processing, failure to fulfill the obligation of cybersecurity data security protection, and other situations.

Considering the nature, duration, harm and situation of Didi's illegal acts, the main basis for the decision of administrative punishment related to the cybersecurity review of Didi is the relevant provisions of the Cybersecurity Law, the DSL, the PIPL and the Administrative Penalty Law etc.

5. Q: What are the key directions and areas of network law enforcement in the next step?

A: In recent years, the state has continuously strengthened the protection of cybersecurity, data security and personal information, and has promulgated laws and regulations such as the Cybersecurity Law, the DSL, the PIPL, the Critical Information Infrastructure Security Protection Regulations, the Cybersecurity Review Measures, and the Data Export Security Assessment Measures. The CAC will strengthen law enforcement in the fields of cybersecurity, data security and personal information protection according to law, and crack down on the harm to national cybersecurity, data security infringement on citizens' personal information and other illegal acts, effectively safeguard national cybersecurity, data security and social public interests, and effectively protect the legitimate rights and interests of the broad masses of the people. At the same time, we should strengthen the exposure of typical cases, form a strong momentum and powerful deterrence, investigate, and deal with a case and give a warning, educate and guide Internet enterprises to operate in accordance with the law, and promote the healthy, standardized and orderly development of enterprises.