


When U.S. Discovery Meets China's New Data and Privacy Laws

Cadence Design Systems, Inc. v. Syntronic AB et al.^[1] (“*Cadence*”) is being recognized as one of the first significant decisions regarding discovery disputes involving Chinese companies claiming that Chinese law, specifically the recently enacted Personal Information Protection Law (“PIPL”), would prevent them from complying with discovery obligations in U.S. proceedings.

Cadence is a patent dispute where the plaintiff, Cadence Design Systems, Inc. (“CDS”), alleged unlicensed use of its software against multiple defendants. In the course of discovery, CDS requested the defendant, Syntronic (Beijing) Technology R&D Center Co., Ltd (“Syntronic Beijing”), to provide several computers that were located in China as part of a discovery request. Syntronic Beijing objected to this, claiming that Chinese data laws and, specifically, the PIPL prevented it from complying with this request.

In subsequent filings by each party's Chinese law experts regarding the discovery dispute, Syntronic Beijing stated that the computers contained personal information, that PIPL article 39^[2] required separate consent of the individuals, and that it could not transfer the computers outside China without it, instead offering to allow CDS to review the computers in China. CDS's expert claimed that PIPL article 13^[3] provided an exception to this—specifically, PIPL article 13(3), which allows for an exception to consent if the request is pursuant to a legal obligation. CDS's expert further claimed that the language of PIPL article 13 regarding exceptions for legal obligations extended to foreign legal obligations, thus encompassing a discovery request for U.S. litigation, and that this exception also extended to the separate-consent requirement found in PIPL article 39. Syntronic Beijing's expert countered by saying that PIPL article 39 is a separate requirement in a separate part of the PIPL and thus separate




consent is required despite the exceptions found in PIPL article 13.

The court held in favor of CDS, finding that the PIPL article 13(3) exception regarding legal requirements can be properly translated as “obligations provided by law” and would encompass foreign legal obligations. The court further found that the exception extended to PIPL article 39, and that separate consent was not required for a cross-border transfer of personal information, in this case the computers. The court held that, therefore, the PIPL was not a bar to the U.S. discovery obligation and ordered Syntronic Beijing to comply with providing the computers to CDS.

This case is significant in that it is one of the very first U.S. courts to deal with the PIPL in the context of a discovery dispute. In this instance, the court interpreted the PIPL and, specifically, separate consent for PIPL article 39 not to create an obstacle for U.S. discovery. While this holding is limited to the Northern District of California, it is significant nonetheless in that it provides a reference point for other courts dealing with a similar issue.

What is interesting here is that neither party raised PIPL articles 38^[5] or 41^[6]. Article 38 requires the transferring party to comply with various requirements prior to the cross-border transfer, while article 41 requires consent from Chinese authorities prior to conducting a cross-border transfer of personal information to a “foreign judicial or enforcement authority,” something the court noted in a footnote. Similar language exists in other Chinese laws, most notably PRC Data Security Law article 36. These clauses could also arguably complicate Chinese parties from complying with discovery obligations abroad and are deserving of closer scrutiny.



In fact, the Ministry of Justice (MOJ) of China in a recent FAQ^[7] has stated it would view this type of cross-border data transfer as a form of international judicial assistance, and advised Chinese parties to seek relevant approvals, conduct security assessments, and comply with requirements under Chinese laws such as the *Civil Procedure Law* and the *Data Security Law* as well as the PIPL. Further complicating the matter is the variety of authorities that would need to give approval in different circumstances. For example, while the MOJ is the authority for approval under The Hague Evidence Convention, the Cybersecurity Administration is charged with regulating and conducting security assessment of data and privacy matters.

While these positions regarding Chinese data security and privacy laws have not been tested significantly in U.S. courts, given this holding in *Cadence*, it is likely coming. Parties to litigation that involves discovery of data, documents, materials, or any information originating in China may run into similar issues. Companies and individuals would be best advised to prepare a comprehensive cross-border discovery strategy ahead of time that can help advance discovery goals while minimizing risks and exposure to Chinese legal and compliance liabilities.

As *Cadence* showed, these strategies and issues hinge on the expertise of Chinese law experts who can work together with their U.S. counterparts. The legal professionals at Winston & Strawn LLP and Yuanda China Law Offices, through their innovative strategic-alliance platform YuandaWinston, are experienced and positioned perfectly to assist in exactly these types of cross-border matters today. Please contact your relationship partner at Winston or Yuanda to learn more.

^[1] Case No. 21-cv-03610-SI (N.D. Cal. June 24, 2022).

^[2] PIPL Art. 39 reads: “Where personal information handlers provide personal information overseas, they shall notify the individuals of matters such as the organizational or personal name and contact methods of the overseas recipient, the purposes and methods of the handling, the types of personal information to be handled, and the methods and procedures for individuals to exercise the rights provided for in this Law, and obtain the individuals’ independent consent.” Translation courtesy of China Law Translate, available at <https://www.chinalawtranslate.com/en/%e4%b8%aa%e4%ba%ba%e4%bf%a1%e6%81%af%e4%bf%9d%e6%8a%a4%e6%b3%95/>.

[3] PIPL Art. 13 reads: "Personal information handlers can only handle personal information where one of the following circumstances is met:

- (1) The individual's consent is obtained;
- (2) As necessary to conclude or perform on a contract to which the individual is a party, or as necessary for carrying out human resource management in accordance with lawfully formulated labor rules systems and lawfully concluded collective contracts;
- (3) As necessary for the performance of legally-prescribed duties or obligations;
- (4) As necessary to respond to public health incidents or to protect natural persons' security in their lives, health, and property in an emergency;
- (5) Handling personal information within a reasonable range in order to carry out acts such as news reporting and public opinion oversight in the public interest;
- (6) For a reasonable scope of handling of personal information that has been disclosed by the individual or otherwise already legally disclosed in accordance with this Law;
- (7) Other situations provided by laws or administrative regulations.

Where the handling of personal information shall be upon obtaining the individual's consent in accordance with other provisions of this Law, but there are circumstances provided for in items 2-7 of the preceding paragraph, the individual's consent is not required to be obtained." Translation courtesy of China Law Translate, available at <https://www.chinalawtranslate.com/en/%e4%b8%aa%e4%ba%ba%e4%bf%a1%e6%81%af%e4%bf%9d%e6%8a%a4%e6%b3%95/>.

[4] PIPL Art. 38 reads: "Where personal information handlers truly need to provide personal information overseas due to business requirements, they shall possess one of the following requirements:

- (1) passing a safety assessment organized by the state internet information departments in accordance with the provisions of Article 40 of this Law;
- (2) Having a professional body conduct personal information protection certification in accordance with provisions of the State Internet Information Departments;
- (3) Contracts concluded with the overseas recipient parties in accordance with standard contract drafted by the state internet information departments agree upon the rights and obligations of both parties,
- (4) Other conditions provided for by laws, administrative regulations, or provisions of the state internet information department.

Where the international treaties and agreements concluded by or participated in by the PRC have requirements for the provision of personal information overseas and so forth, those provisions may be implemented.

Personal information handlers shall employ necessary measures to ensure that the overseas recipients' activities handling personal information meet the protection standards provided for personal information provided for in this Law."

[5] PIPL Art. 41 reads: "The competent organs of the PRC are to handle requests for the provision of domestically stored personal information from foreign justice or law enforcement based on relevant laws and international treaties and agreements concluded or participated in by the PRC, or in accordance with the principle of reciprocity. Those handling personal information must not provide personal information stored within the PRC to foreign justice or law enforcement bodies without the permission of the

competent organs of the PRC.” Translations courtesy of China Law Translate, available at <https://www.chinalawtranslate.com/en/%e4%b8%aa%e4%ba%ba%e4%bf%a1%e6%81%af%e4%bf%9d%e6%8a%a4%e6%b3%95/>

[6] *PRC Data Security Law* Art. 36 reads: “The competent organs of the PRC are to handle requests for the provision of data from foreign justice or law enforcement based on relevant laws and international treaties and agreements concluded or participated in by the PRC, or in accordance with the principle of reciprocity. Domestic organizations and individuals must not provide data stored within the PRC to foreign justice or law enforcement bodies without the permission of the competent organs of the PRC.” Translation courtesy of China Law Translate, available at <https://www.chinalawtranslate.com/en/datasecuritylaw/>.

[7] http://www.moj.gov.cn/pub/sfbgw/jgsz/jgszzsdw/zsdwsfxzjlzx/sfxzjlzxxwdt/202206/t20220624_458335.html

Authors



Ya-Chiao Chang

Partner, Yuanda

Shanghai

+86 21 2208 2628

ychang@winston.com