MEALEY'S®

Data Privacy Law Report

China's New Privacy and Data Security Statutes Further Complicate U.S. Litigations

by

Don Z. Wang
Axinn, Veltrop & Harkrider LLP
San Francisco, CA

Brooke J. Oppenheimer
Axinn, Veltrop & Harkrider LLP
Hartford, CT

and

Shawn Lee
Intellectual Property Institute of Xiangtan University
Institute for Studies on Artificial Intelligence and Law of Tsinghua University
Beijing, China

A commentary article reprinted from the February 2022 issue of Mealey's Data Privacy Law Report

LexisNexis®

Commentary

China's New Privacy and Data Security Statutes Further Complicate U.S. Litigations

By
Don Z. Wang,
Brooke J. Oppenheimer
and
Shawn Lee

[Editor's Note: Don Z. Wang is an Associate attorney in Axinn, Veltrop & Harkrider LLP's Intellectual Property Group counseling technology and pharmaceutical companies in complex patent and antitrust litigations. Brooke J. Oppenheimer is an attorney in Axinn's Complex Litigation and Antitrust Litigation Groups working with firm and corporate clients to ensure compliance with the rapidly developing data, privacy and security laws. Shawn Lee is an adjunct professor at the Intellectual Property Institute of Xiangtan University and a research fellow of the Research on the Legal-based Governance of Internet Economy Project at the Institute for Studies on Artificial Intelligence and Law of Tsinghua University. Any commentary or opinions do not reflect the opinions of Axinn, Veltrop & Harkrider LLP, Xiangtan University, Tsinghua University, or LexisNexis®, Mealey Publications™. Copyright © 2022 by Don Z. Wang, Brooke J. Oppenheimer, and Shawn Lee. Responses are welcome.]

Introduction

In the fall of 2021, China enacted two statutes with broad implications for a wide range of data processing activities both in and out of China: Data Security Law ("DSL") and Personal Information Protection Law ("PIPL"). Among other impacts, each statute's respective "blocking provision" introduces new complications to a company's litigation efforts in the United States if any data relevant to such a litigation is stored in China.

DSL, which was enacted on June 10, 2021 and took effect on September 1, 2021, "applies to data handling activities and their security regulations within the mainland territory of the People's Republic of China (PRC)" as well as "data handling activities outside the mainland territory of the PRC [that] harm the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC."[1] "Data" is broadly defined as "any information record in electronic or other form[s]."[2] Similarly broad, the term "'[d]ata handling' includes the collection, storage, use, processing, transmission, provision, disclosure, etc., of data."[3]

PIPL, which was enacted on August 20, 2021 and took effect on November 1, 2021, is widely considered China's version of Europe's GDPR.[4] PIPL "applies to the activities of handling the personal information of natural persons" within PRC as well as such activities outside of PRC if they target natural persons within PRC.[5] "Personal information" is broadly defined as "all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling."[6] Similar to "data handling" in DSL, "personal information handling" under PIPL encompasses the "collection, storage, use, processing, transmission, provision, disclosure, deletion, etc." of personal information.[7]

Given their broad language, both statutes could apply to many aspects of the e-discovery process that is a typical part of a U.S. litigation or investigation, such

as preservation/litigation hold, collection, review, cross-border transfer to the U.S., and production, if any relevant data is originally stored in China or includes personal information of people in China. Particularly relevant to such U.S. litigations, each statute includes a "blocking provision" prohibiting companies from providing data or personal information to foreign judicial or law enforcement agencies without PRC authorities' prior approval.

Blocking Provisions of DSL and PIPL

Article 41 of PIPL provides:

> Competent authorities of the People's Republic of China, according to relevant laws and treaties or international agreements that the People's Republic of China has concluded or acceded to, or according to the principle of equality and mutual benefit, are to handle foreign judicial or law enforcement authorities' requests regarding the provision of personal information stored domestically. Without the approval of the competent authorities of the People's Republic of China, personal information handlers may not provide personal information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies.[8]

Article 36 of DSL includes a nearly identical prohibition for the provision of any "data stored within the mainland territory of the PRC" to such foreign judicial or law enforcement authorities without the prior approval of relevant authorities of China.[9] Of course, the DSL provision has a significantly wider scope as it is not limited to "personal information." Violation of these provisions may result in severe fines to the violating company (up to 5 million RMB under DSL and up to 50 million RMB or 5% of annual revenue under PIPL) as well as the suspension of relevant business licenses or permits.[10] Furthermore, relevant management personnel who are "directly responsible" can be held personally liable for a fine (up to 500,000 RMB under DSL and 1 million RMB under PIPL) as well as prohibition from holding relevant positions for a certain period of time.[11]

These blocking provisions are generally understood to prohibit directly providing information to a foreign court (e.g., court filings, presenting at a court hearing, or submission for in camera review) or any law enforcement/prosecutorial agency (in a criminal investigation or litigation). The extent to which these provisions apply to discovery in U.S. civil litigation context is not entirely clear. In China, discovery efforts in civil litigations are generally organized and ordered by the courts, thus any production of information in such a civil case would constitute providing information to the court. Discovery in a U.S. civil litigation involves the exchange of information between private parties, but the court still plays a supervisory role in adjudicating discovery disputes, which can involve reviewing certain underlying information or documents. Further, the information exchange in U.S. discovery is typically conducted with an expectation that some of the exchanged information will end up being presented in court. Whether the supervisory role played by the court and the expectation of the eventual presentation in court would trigger the prohibition outlined in DSL Article 36 and PIPL Article 41 remains unanswered as the regulation promulgation efforts are ongoing. But this ambiguity creates risk for litigants whose information is covered by DSL and PIPL.

Comparison to Prior Statutes' Blocking Provisions

DSL and PIPL were not the first PRC statutes to include this type of blocking provisions. At least the following previously enacted statutes include blocking provisions similar to those of DSL and PIPL in certain respects:

• ***Law of the PRC on Guarding State Secrets***: Articles 25 and 48 prohibit any individual or entity from carrying or transferring any medium containing state secrets out of China without the approval of relevant PRC authorities.[12]

• ***Cybersecurity Law***: Article 37 requires a critical information infrastructure operator to conduct a security assessment as promulgated by the relevant PRC authorities before transferring any critical data and personal information out of China.[13]

• ***International Criminal Judicial Assistance Law***: Article 4 prohibits any individual or entity in China from providing evidentiary materials or assistance to foreign countries without the approval of relevant PRC authorities.[14]

• ***Securities Law***: Article 177 prohibits any individual or entity in China from providing documents and materials relating to securities business activities to foreign countries without the approval of relevant PRC authorities.[15]

However, these prior statutes generally focused on information and industries widely considered critical to PRC's national security or overall economy, such as companies handling state secrets, critical information infrastructure operators, banking industry, and key securities market players. Accordingly, the companies implicated by these prior statutes are often state-owned or state-affiliated enterprises, or companies that receive considerable amount of support from various levels of PRC governments.

In contrast, DSL and PIPL both apply to economic sectors substantially broader than those implicated by prior statutes. In particular, both DSL and PIPL have significant implications on digital economy, such as social media or e-commerce companies. As a result, the vast majority of the entities implicated by DSL and PIPL are likely private companies that do not enjoy the same type of close relationship with the PRC government as those "critical industries" implicated by prior blocking statutes.

Complications to U.S. Litigation Efforts

These blocking provisions of DSL and PIPL introduce new complications for companies with data stored in China that is also relevant to ongoing U.S. litigations or governmental investigations. Companies in this situation will likely be caught in the dilemma of attempting to comply with conflicting orders issued from PRC authorities and U.S. courts, and may even subject themselves to both the penalties outlined in these statutes and Rule 37 discovery sanctions issued by the U.S. courts.

Companies seeking to rely on these blocking provisions to resist production in U.S. litigation face an extremely high hurdle. Generally, the party invoking a foreign blocking statute has the burden not only to assert the basis for its objections with particularity under Rule 26(b)(5)(A) of Federal Rules of Civil Procedure, but must also prove in accordance Rule 44.1 that it is constrained by a foreign statute that indeed applies to the discovery sought and conflicts with U.S. production requirements.[16] If such a conflict is established, courts apply a multi-factor "comity analysis" endorsed by the U.S. Supreme Court in its *Societe Nationale Industrielle Aerospatiale v. U.S. District Court* to determine whether the blocking statute excuses a resisting party's noncompliance with its production obligations.[17] Specifically, citing to the Restatement (Third) of Foreign Relations Law § 442(1)(c), the U.S. Supreme Court outlined five factors in *Aerospatiale*:

• the importance to the litigation of the documents or other information requested;
• the degree of specificity of the request;
• whether the requested information originated in the United States;
• the availability of alternative means of securing the information; and
• balancing of the national interests of the United States and the foreign country at issue in the compliance or noncompliance with the discovery obligations.[18]

As these factors are non-exhaustive, lower courts further developed additional factors to aid the analysis:[19]

• the hardship of compliance on the party or witness from whom discovery is sought;
the good faith of the party resisting discovery; and
• the likelihood of compliance if the objection is overruled.

Past attempts to resist production in U.S. litigations based on prior PRC statutes' blocking provisions have rarely succeeded. For example, the Ninth Circuit in *Richmark* rejected a PRC state-affiliated entity's effort to resist production based on prohibitions specified in PRC's state secrecy law.[20] The D.C. Circuit in *In re Sealed Case* similarly held that the potential penalties under PRC's International Criminal Judicial Assistance Law do not excuse noncompliance with the district court's discovery orders.[21] Various district courts also rejected efforts of resisting production based on various provisions in PRC's banking laws and general civil procedure laws.[22] In fact, one district court has already applied *Aerospatiale*'s comity analysis on both DSL and PIPL in anticipation of such arguments to be raised by the resisting party and concluded that these statutes, like PRC's state secrecy laws, would not excuse noncompliance with the party's discovery obligations.[23]

Notably, the court in *In re Valsartan* expressed doubts as to whether these blocking provisions of DSL and PIPL, along with other blocking statutes, actually define any vial national interest "with particularity" as opposed to merely providing an ad-hoc justification for resisting unfavorable discovery.[24] Both DSL and PIPL identify the protection of lawful rights and interests of individuals and organizations as the key national interests underlying the statutes.[25] DSL additionally identifies safeguarding "national sovereignty, security, and development interests" reflecting a "data sovereignty" approach, which can often be perceived as overly protective by foreign jurisdictions.[26] The court in this case speculated that such blocking statutes merely "serve to justify nondisclosure of any information a PRC governmental agency wants to keep out of U.S. litigation" as they appear to be "a sword of Damocles to keep international business in line but infrequently wielded if ever against a titan of the PRC economy."[27]

Relatedly, in analyzing the hardship of compliance imposed by the prior PRC blocking statutes, courts often described the potential penalties faced by the resisting entities as "speculative at best."[28] In so observing, courts expressed doubt as to whether these companies would face serious repercussions for violating the relevant blocking provisions as they are either state-owned/state-affiliated entities or play a key role in China's overall economy.[29] It is highly questionable if these assumptions hold true for many companies affected by the blocking provisions in DSL and PIPL. As discussed above, unlike the prior blocking statutes, DSL and PIPL have substantially broader applicability, and more likely would implicate technology, e-commerce, and social media companies. In recent years, companies in these sectors have been subject to increasing scrutiny from the PRC government.[30] For example, it is widely observed that various PRC regulatory agencies took a series of enforcement actions against Didi Chuxing, a ride-hailing leader in China, merely a month after the enactment of DSL in 2021.[31] Commentators further observed that Didi's oversea IPO activities may have triggered PRC government's concerns over its likely sharing of data with foreign securities regulators for compliance audits.[32]

Even if an implicated company is able to obtain PRC authorities' approval to produce relevant data in U.S. litigations, the lengthy delay may nonetheless hamper the company's ability to properly respond to data requests and defend itself. For example, in a criminal trade secret case against a Chinese semiconductor manufacturer, the defendant was forced to request an extension for making reciprocal discovery disclosure under Rule 16(b)(1)(A) of the Federal Rules of Criminal Procedure as the requested documents were under PRC government's review pursuant to the blocking provisions of DSL, PIPL, and the International Criminal Judicial Assistance Law.[33] In its briefing, the defendant argued that the subject documents include "important, potentially exculpatory evidence" and it would be substantially prejudiced if the deadline is not extended to accommodate the delay.[34] This is further complicated by the lack of guidance on how to obtain approval to produce information to foreign judicial or law enforcement agencies under DSL or PIPL, and whether separate approval paths are required for each statute.

Best Practices to Navigate Blocking Statues in U.S. Litigations

While the exact approach to best navigate the potential conflicts created by DSL, PIPL, and other blocking statutes in a U.S. litigation will vary from case to case and will likely need to be adjusted based on the eventual regulations promulgated, certain general strategies may nonetheless help practitioners to minimize related risks and disruptions.

• Be Mindful of Where to Store Relevant Data

The best way to solve a problem may be to prevent the problem from happening in the first place. Article 36 of DSL and Article 41 of PIPL are generally limited to data and/or personal information "stored within the mainland territory of PRC."[35] If a company anticipates habitual litigation in the U.S., the company should consider the location of its data servers and storage facilities as the conflict between DSL and PIPL with the U.S. discovery process will be a constant hardship.

• Understand the Company's Data Map

In order to adequately prepare for potential future litigation, companies need to have a comprehensive understanding of the various data systems, formats, and contextual classifications of information utilized in their business operations. Further, it will be helpful for a company to understand how its data flows in

and out of China in order to determine if other non-China sources of data exist.

- **Prepare a Litigation Commencement Plan**

As parties have an obligation to preserve potentially relevant information when litigation is "reasonably anticipated," companies should work with their counsel to develop a plan to determine (1) how to identify potentially relevant data, (2) how to preserve potentially relevant data, and (3) a plan to obtain permission from the relevant "competent authorities of the People's Republic of China" or a manner to determine such permission is not needed for a given data set. As discussed, the DSL and PIPL address the "collection, **storage**, use, **processing**, transmission, provision, disclosure, deletion, etc." of data which covers the preservation and holding of data for the purpose of litigation.[36] Unfortunately, U.S. discovery rules give parties very little leeway to implement a "litigation hold" upon a reasonable expectation of litigation.[37]

- **Identify and Disclose Potential Blocking Statutes/Regulations Early in Discovery**

Once a litigation starts, the process of identifying relevant blocking statutes and related regulations should start as soon as there is a reasonably belief that any data may need to be produced from China. As discussed below, the universe of related regulations for such blocking statutes can be extensive and time-consuming to navigate. Further, the existence of such blocking statutes and regulations, as well as the substantive requirements imposed, should be disclosed to the opposing party and the court as early as possible to help shape the discovery scope, process, and timeline, as well as to show good faith cooperation in the discovery process. Ideally, the issue can be discussed in the Rule 26 conference between the parties and the initial Rule 16 conference with the court. If possible, practitioners should also consider referencing and even incorporating specific blocking statutes and regulations in the applicable scheduling orders, discovery order, ESI order, and/or protective order to create a trail of written record for elevating such issues.

- **Preserve Related Objections and Leverage the Likely Burden to Narrow the Discovery Scope**

While resisting production entirely is unlikely to succeed, courts may nonetheless recognize the extraordinary burden imposed on a company by such blocking statutes and substantially narrow the discovery scope accordingly.[38] Practitioners intending to leverage such potential burden in this manner must properly preserve the objections during the discovery process (e.g., written objections, meet & confers, and even motion practices).[39]

Identify Specific Instances of Sanctions Imposed Under the Blocking Statutes to Demonstrate Burden/Hardship

Practitioners should try to be as specific as possible when trying to make the burden/hardship arguments during a discovery dispute. Past cases have demonstrated that court view the hardship imposed by such blocking statutes as speculative tend to be more receptive to the argument when a resisting party can identify specific cases where an entity was sanctioned under the cited statutes.[40] Further, practitioners should also document the time, costs, and resources involved in the efforts to comply with these blocking statutes to further support a hardship argument.

- **Closely Monitor the Development of Corresponding Regulations**

While DSL, PIPL, and the 2017 Cybersecurity Law are collectively described as the "Three Horse Carriages" of China's data protection and cybersecurity regime, they primarily provide an outline or overall "architecture" for such a regime. The exact obligations a company may face will largely be determined by various regulations and agency rules currently being promulgated. Accordingly, practitioners should closely monitor the development of corresponding regulations. The universe of relevant regulations can extensive and difficult to navigate. Some of the key regulations to watch include the Cybersecurity Review Measures,[41] Outbound Data Transfer Security Assessment Measures (Draft for Comment),[42] and Online Data Security Management Regulations (Draft for Comment),[43] Further, there are certain "pilot" regulations being experimented in specific industries, such as the Industrial and Information Sectors Data Security Management Measures (Trial) (Draft for Comment)[44] and the Several Provisions on the Admin-

istration of Automobile Data Security (Trial),[45] which will likely further influence the direction of the overall regulation activities. ■

Endnotes

1. Data Security Law of PRC (2021), Article 2. Original texts published by PRC's National People's Congress are available at http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml. English translation provided by Stanford University's DigiChina Project is available at https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.
2. DSL Article 3.
3. *Id*.
4. Personal Information Protection Law of PRC (2021). Original texts published by PRC's National People's Congress are available at http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml. English translation provided by Stanford University's DigiChina Project is available at https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.
5. PIPL, Article 3.
6. PIPL, Article 4.
7. *Id*.
8. PIPL, Article 41.
9. DSL, Article 36.
10. DSL, Article 48; PIPL, Article 66.
11. DSL, Article 48; PIPL, Article 66.
12. Law of the PRC on Guarding State Secrets (Amended in 2010), Articles 25 and 48. Original texts published by the Central People's Government of the PRC are available at http://www.gov.cn/flfg/2010-04/30/content_1596420.htm.
13. Cybersecurity Law of PRC (2017), Article 37. Original texts published by the Cyberspace Administration of China are available at http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.
14. International Criminal Judicial Assistance Law (2018), Article 4. Original texts published by the National People's Congress of the PRC are available at http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-10/26/content_2064576.htm.
15. Securities Law of PRC (Amended in 2019), Article 177. Original texts published by the Central Government of the PRC are available at http://www.gov.cn/xinwen/2019-12/29/content_5464866.htm.
16. *In re Valsartan, Losartan, & Irbesartan Prods. Liab. Litig.*, MDL No. 2875 (RBK), 2021 U.S. Dist. LEXIS 242593, at *137-38 (D.N.J. Dec. 20, 2021).
17. 482 U.S. 522 (1987).
18. *Id*. at 544 n.28.
19. *Richmark Corp. v. Timber Falling Consultants,* 959 F.2d 1368, 1475 (9th Cir. 1992); *Wultz v. Bank of China Ltd.*, 910 F. Supp. 2d 548, 553 (S.D.N.Y. 2012).
20. *Rickmark*, 959 F.2d at 1471; *see also Munoz v. China Expert Tech., Inc.*, 07 Civ. 10531(AKH), 2011 U.S. Dist. LEXIS 128586, at *3-7 (S.D.N.Y. Nov. 7, 2011); *In re Valsartan*, 2021 U.S. Dist. LEXIS 242593, at *157-60.
21. *In re Sealed Case*, 932 F.3d 915, 918 (D.C. Cir. 2019).
22. *See e.g.*, *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1956 and 50 U.S.C. § 1705*, 381 F. Supp. 3d 37 (D.D.C. 2019); *Mikiken & Co. v. Bank of China*, 758 F. Supp. 2d 238 (S.D.N.Y. 2010); *Wultz*, 910 F. Supp. 2d at 561.
23. In re Valsartan, 2021 U.S. Dist. LEXIS 242593 at *129-37, 157-64.
24. *Id*. at *145-46, 157-58.
25. DSL, Article 1; PIPL, Article 1.
26. DSL, Article 1; Roxana Vatanparast, *Data Governance and the Elasticity of Sovereignty*, 46 Brooklyn J. Int'l L. 1, 16-17, 30 (2020).
27. *In re Valsartan*, 2021 U.S. Dist. LEXIS 242593 at *145, 155,
28. *Milliken*, 758 F. Supp. 2d at 250; *Tiffany (NJ) LLC v. Forbse*, 11 Civ 4976 (NRB), 2012 U.S. Dist. LEXIS 72148, at *27-28 (S.D.N.Y. May 23, 2012).
29. *In re Grand Jury*, 381 F. Supp. 3d at 42; *Tiffany,* 2012 U.S. Dist. LEXIS 72148 at *27-28.
30. *See e.g., China Fines Alibaba $2.8 Billion in Landmark Antitrust Case*, New York Times (Sept. 1, 2021), available at https://www.nytimes.com/2021/04/09/

technology/china-alibaba-monopoly-fine.html; *China's E-Commerce Crackdown: Timeline of Beijing's Action to Bring Tech Giants in Line with National Policy*, South China Morning Post (Nov. 22, 2021), available at https://www.scmp.com/tech/policy/article/3156719/chinas-e-commerce-crackdown-timeline-beijings-actions-bring-tech-giants; C*hina's Tech Crackdown: A Year-in-Review,* Hard National Security Choices (Jan. 7, 2022), available at https://www.lawfareblog.com/chinas-tech-crackdown-year-review.

31. *In the New China, Didi's Data Becomes a Problem*, Wall Street Journal (July 18, 2021), available at https://www.wsj.com/articles/in-the-new-china-didis-data-becomes-a-problem-11626606002.

32. *See e.g., How Didi Crashed I nto China's New Data Security Law*, TCG (Oct. 28, 2021), available at https://thechinaguys.com/didi-security-data-law-chuxing-china-tech-stock/.

33. Defendant's Fujian Jinhua's *Ex Parte* Application to Extend Deadline for Jinhua to Make it Reciprocal Disclosures Under Rule 16(b)(1)(A), *United States v. Fujian Jiinhua Integrated Circuit, Ltd.*, Case No. 3:18-cr-00465, ECF No. 232 (N.D. Cal. Nov. 18, 2021).

34. *Id*. at 5.

35. DSL, Article 36; PIPL, Article 41.

36. DSL, Article 3; PIPL, Article 4 (emphasis added).

37. *See e.g., Bagley v. Yale Univ.*, 318 F.R.D. 234 (D. Conn. Dec. 22, 2016) (holding that duty to preserve arose before filing of suit and arguably when the university staff exchanged emails noting plaintiff's threat of legal actions, thus the university's litigation hold issued months after such threats may support a spoliation claim).

38. *Ney v. Ownens-Illinois, Inc.*, Case No. 16-cv-2408, 2016 U.S. Dist. LEXIS 169371, at *12, 14-16 (E.D. Pa. Dec. 6, 2016) (finding that, though Quebec's blocking statute does not excuse the defendant from non-production, the plaintiff's requests are overly broad under *Aerospatiale*'s factor two analysis and need to be substantially narrowed).

39. *Richmark*, 959 F.2d 1374 (finding that the defendant has waived its objection based on PRC's secrecy law since it failed to raise such an objection to plaintiff's discovery request).

40. Compare Nike, Inc. v. Wu, 349 F. Supp. 3d 310 (S.D.N.Y. 2018) ("[T]he Bank[s] ha[ve] cited no specific instance in which a Chinese financial institution was punished for complying with a foreign court order directing the production of documents") with *Tiffany (NJ) LLC v. Andrew,* 276 F.R.D. 143, 158 (S.D.N.Y. 2011) ("Unlike Milliken, the Banks here have cited Chinese cases in which a commercial bank was held liable to its customer after turning over the individual's funds or information to a third party.")

41. Cybersecurity Review Measure (Dec. 28, 2021). Original texts published by the Cyberspace Administration of China are available at http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm.

42. Outbound Data Transfer Security Assessment Measures (Draft for Comment) (Oct. 29, 2021). Original texts published by the Cyberspace Administration of China are available at http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm. English translation provided by Stanford University's DigiChina Project is available at https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/.

43. Online Data Security Management Regulations (Draft for Comment) (Nov. 14, 2021). Original texts published by the Cyberspace Administration of China are available at http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm. English translation provided by Stanford University's DigiChina Project is available at https://digichina.stanford.edu/work/translation-online-data-security-management-regulations-draft-for-comment-nov-2021/.

44. Industrial and Information Sectors Data Security Management Measures (Trial) (Draft for Comment) (Sept. 30, 2021). Original texts published by the Ministry of Industry and Information Technology of PRC are available at https://wap.miit.gov.cn/gzcy/yjzj/art/2021/art_dcb6cc8d9f5c414eabd7070871996525.html.

45. Several Provisions on the Administration of Automobile Data Security (Trial) (Aug. 20, 2021). Original texts published by the Cyberspace Administration of China are available at http://www.cac.gov.cn/2021-08/20/c_1631049984897667.htm. ■

MEALEY'S DATA PRIVACY LAW REPORT
edited by Mark Rogers
The Report is produced monthly by

11600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: http://www.lexisnexis.com/mealeys