IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY
CAMDEN VICINAGE

IN RE VALSARTAN, LOSARTAN, AND IRBESARTAN PRODUCTS LIABILITY LITIGATION	:	MDL No. 2875 (RBK) and Special Master Honorable (Ret.) Thomas Vanaskie
	:	**OPINION and ORDER RE:** ZHP PARTIES' MOTION TO VACATE SPECIAL MASTER ORDER NO. 35 (Doc.1482)
This Document Relates To All Actions.	:	

KUGLER, United States District Judge:

Before the Court in this Multi-District Litigation ["MDL"] that concerns the sale in the U.S. of generic, prescription Valsartan pharmaceuticals, found by the Food and Drug Administration ["FDA"] to contain cancer-causing contaminants, is Defendant ZHP Parties'[1] motion to vacate ["the motion"] (Doc. 1550) Special Master Order No. 35 ["SMO 35"] (Doc. 1482) under Fed. R. Civ. Proc. ["FRCP" or "Rule"] 53(f).

Specifically, SMO 35 dated 12 Aug 2021 compelled production of 20 documents while denying production of 3 documents, finding they likely contained state secrets under the *Law of the PRC on Guarding State Secrets* ["the PRC State Secret Law" or "SSL"].

HAVING REVIEWED ZHP's brief (Doc. 1550-1), plaintiffs' opposition (Doc. 1570), and ZHP's reply (Doc.1583) without a hearing in accordance with Local Rule ["LR"] 78.1 (b), and for the reasons stated below, and for good cause shown:

THE COURT:

DENIES ZHP's motion to vacate SMO 35; and

AFFIRMS SMO 35 in its entirety; **and**

ORDERS:

Plaintiffs' Motion To Compel (Doc. 1231) is **GRANTED IN PART AND DENIED IN PART**;

[1] Zhejiang Huahai Pharmaceutical Co, Ltd., Huahai U.S., Inc., Prinston Pharmaceutical Inc., and Solco Healthcare US, LLC collectively are termed herein ZHP.

and FURTHER ORDERS:

by the next Case Management Conference ["CMC"] in this MDL scheduled to occur on 5 Jan 2022, ZHP shall produce all documents that are the subject of Plaintiffs' Motion to Compel, along with all documents listed as duplicates of these documents on its State Secrets Review Log of documents withheld as Chinese state secrets, with the exception of the following three documents and any duplicates of the following three documents: ZHP0255672, ZHP02622051, and ZHP02622054;

and FURTHER ORDERS

the 20 documents affirmed here as discoverable shall be disclosed to plaintiffs in the same format (i.e., redacted or original) as ordered in SMO 35;

and **only to select** members of plaintiffs' executive committee ["PEC"] having an immediate need to know, as determined by Plaintiffs' Lead Counsel (*See Case Management Order No.* 6, Doc. 96);

the PEC shall create and maintain a Disclosure Log from the date of the next CMC, which in real time records and archives disclosure details, that is, which attorneys of the PEC have been given access; what document(s); and the date of disclosure;

PEC attorneys who have been given access to any document(s) on the State Secret Review Log shall adopt best practices to maintain the secrecy and confidentiality of the document(s);

no member of the PEC nor other of plaintiffs' attorneys shall distribute, disclose, or recite any, or any portion, of these 20 disclosed documents to other plaintiffs' attorneys who are not members of the PEC without first making a motion for such disclosure to the Special Master for exceptional cause; and

if the Special Master allows disclosure to other plaintiffs' attorneys, then the PEC shall update in real time the Disclosure Log.

1.0 Facts and Background

The Court refers the reader to SMO 35 for a full exposition of the facts and background to the motion and gives a pared down summary here. This is a discovery dispute about whether any of 23 ZHP documents created in the PRC are state secrets under the SSL and, if

so, whether the SSL therefore regulates their non-disclosure in this litigation. The distilled point of contention is whether the Federal Rules of Civil Procedure, especially Rule 26—to give a just and transparent determination of every action and proceeding in U.S. civil litigation—overrides or not the presumed prohibition under the SSL of the disclosure of these documents. Specifically, at issue are fourteen (14) documents that ZHP has provided plaintiffs in redacted form and nine (9) documents withheld in their entirety.

This dispute has been ongoing for over a year, with ZHP sequentially reducing the number of documents withheld as Chinese state secrets from the original 335 to 91 and then to the disputed 23. Exacerbating the dispute is the Catch-22 that, in order to abide by the SSL, ZHP U.S. attorneys have given plaintiffs a State Secret Review Log ["Secret Log"] of the withheld documents without personally reviewing the documents themselves. The ZHP U.S. attorneys have relied on various Chinese law firms to summarize the contents of the withheld documents and analyze whether the SSL actually does prohibit their disclosure. ZHP maintains that neither its U.S. attorneys nor the Court may review the documents personally, else, if the documents do contain Chinese state secrets, that review would violate the SSL. The successive reduction of the Secret Log to 23 withheld documents stems from ZHP's engagement of three Chinese law firms which, in their separate reviews, have re-categorized successively fewer and fewer documents as possibly implicating the SSL, and suggesting at the same time that some of the documents could be produced, if redacted.

On 10 May 2021, plaintiffs filed a motion to compel the production of the 23 documents on the Secret Log. Doc. 1231 and accompanying brief at Doc. 1231-1. On 12 May 2021, ZHP timely filed its opposition brief (Doc. 1267) to plaintiffs' motion to compel as well as a cross motion for a protective order (Doc.1268) precluding the production of the documents withheld on the Secret Log, which relied on the arguments in its opposition. On 12 August 2021, in Doc. 1482 ["SMO 35"], the Special Master ruled 20 of the 23 documents could be produced with the condition that 14 of the documents remain redacted. On 8 September 2021, ZHP filed the instant motion to vacate SMO 35. Doc. 1550 and accompanying brief at 1550-1. On 20 September 2021, plaintiffs timely filed their opposition (Doc. 1570) to which ZHP timely replied on 27 September 2021 in Doc. 1583.

A primary procedural concern here is the lack of transparency and guidance in the SSL

(and its Regulations) as to how a PRC defendant could recognize with a degree of confidence whether any information it was producing was a state secret under the SSL and the liability attached to that disclosure. Several U.S. legal pundits have remarked this endemically vague definition of a "state secret" in the SSL provokes in PRC defendants a somewhat unavoidable anxiety, and therefore deep disincentive, to produce in U.S. litigation information even remotely implicating the SSL.[2] A theme in Federal Court litigation is that PRC defendants, when in doubt as to their potential liability for the production of PRC state secrets, invoke the SSL and don't produce.[3] In effect, the uncertainty as to what a PRC state secret is can work to

---

[2] Jerry C. Ling, *Traps for the Unwary in Disputes Involving China*, JONES DAY COMMENTARIES, August 2012 https://www.jonesday.com/en/insights/2012/08/traps-for-the-unwary-in-disputes-involving-china (last accessed 10 Dec 2021); Rocky T. Lee, *New Laws In China Regarding "State Secrets" and Related Issues*, CADWALADER CLIENTS & FRIENDS MEMO, May 2011, https://www.google.com/search?client=firefox-b-1-d&q=concern+over+the+2010+PRC+law+on+guarding+state+secrets (last accessed 10 Dec 2021); Mitchell A. Silk & Jillian S. Ashley, Understanding China's State Secrets Laws, CHINA BUSINESS REVIEW, 1 Jan 2011 https://www.chinabusinessreview.com/understanding-chinas-state-secrets-laws/ (last accessed 14 Dec 2021).

[3] Précised below are fairly typical U.S. federal court cases in which PRC defendants have asserted their liability under the SSL for not disclosing certain information located in the PRC. These are by no means the only cases where PRC defendants have asserted the SSL(or other PRC blocking statutes) to ground non-disclosure. In fact, the more research the Court has done, the more such cases have turned up. In no particular order, the first three cases, (1) to (3),below exemplify discovery decisions by Magistrate Judges; the next cases, (4) to (6), are District Court discovery decisions involving the SSL.

Magistrate Judge Decisions.

In each of these, a Magistrate Judge ruled that either the PRC's interest in preserving the "state secret" was not shown with evidentiary credulity and/or there was no reliable, direct decision by a PRC government entity that withheld information comprised a PRC state secret. In some, the District Judge was called upon to review.

1) Meggitt (Orange County), Inc. v. Nie Yongzhong, No. SACV 13–0239–DOC (DFMx), 2015 WL 1809354 at *7-8 (C.D. Cal. 21 Apr 2015). This citation is to the District Judge's affirmance of the Magistrate's decision in a trade secret misappropriation case where a PRC defendant invoked the SSL to prevent discovery of technical information relevant to the theft of plaintiffs' designs. The Magistrate Judge ruled the defendant was overreaching in its invocation of the SSL:

> *"[A] balancing of the Richmark factors weighs in favor of ordering Defendants to produce the discovery about which they assert the applicability of China's state secrets law. This result is particularly warranted in light of (1) Defendants' failure to demonstrate an actual likelihood that production would result in criminal or civil liability in the PRC,*
> *(2) the United States's interest in providing a remedy for the clear harm caused by trade secret misappropriation to parties like Plaintiff, and*
> *(3) the Court's skepticism about the validity of PRC's interest in preventing disclosure."* Id. at * 8.

2) Masimo Corporation v. Mindray DS USA, Inc., No. SACV 12-02206-CJC (JPRx)2014 WL 12597116, at *2 (C.D. Cal. 15 Apr 2014). Again, involving trade secret misappropriation, but of software code. This citation is to the District Judge's denial to review the Magistrate's decision that the relevant source code must be produced, **even though the PRC government had ruled the source code was subject to the SSL.**

3) Autodesk, Inc. v. ZWCAD Software Co., Ltd. et al., 5:14-cv-01409-EJD, 2015 WL 1928184, at *((N.D. Cal. 27 Mar 2015). Also, involving trade secret theft, PRC defendant ZWSoft, like the defendant in *Aérospatiale* (*See infra*), moved to require Autodesk to conduct all discovery pursuant solely to the Hague Convention rather than through the Federal Rules **to mitigate any possible risk that discovery of its data and documents outside of the PRC would subject defendant to liability under the SSL and the PRC's privacy laws**. The Magistrate denied the motion because ZWSoft had not shown a genuine / reliable risk of liability under the SSL. *See also*, *Autodesk, Inc. v. ZWCAD Software Co., Ltd. et al.*, No. 5:14-cv-01409-EJD, 2015 WL 2265479114 (N.D. Cal. 13 May 2015) [where the District Judge discusses the Magistrate's decision].

District Judge Decisions

4) Wultz v. Bank of China Ltd., 942 F.Supp.2d 452, 466 - 473 (S.D.N.Y. 2013). In a case involving a suicide bombing attack in Israel that killed and wounded U.S. citizens, U.S. plaintiffs brought suit against the PRC-owned Bank of China (BOC) for its financial support of anti-Israel terrorist agencies. Plaintiffs argued that support fostered the attack and moved to compel BOC's records of certain bank accounts that had transferred funds to anti-Israel terrorist organizations. BOC sought a protective order to prohibit discovery, citing the SSL among other PRC laws. In resolving the motions, **the District Judge recognized the motion to compel was most likely in contravention of PRC law, especially since BOC was a state-owned enterprise ["SOE"]**. In performing a balancing analysis of the *Aérospatiale* factors, the Court concluded that, since to some extent BOC's behavior during discovery showed elements of bad faith, the motion to compel was in part granted. The Court reasoned that if the case were resolved BEFORE TRIAL, there would be NO reasonable basis for the disclosed documents to become public. In that situation, only the attorneys and the Court will have seen the documents, which would limit their exposure outside of the PRC. Thus, the District Judge's balancing analysis of the U.S. and PRC interests attempted to find a way to limit liability for BOC, notwithstanding the finding of BOC's bad faith.

5) Munoz v. China Expert Technology, Inc., No. 07 Civ. 10531 (AKH), 2011 WL 5346323 (S.D. N.Y. 7 Nov 2011). Plaintiffs cite this case in their brief, but *Munoz* does not exemplify an actual *Aérospatiale* balancing as the *Munoz* defendant, incorporated in the U.S., was subject to the discovery injunctions of the FRCP. Nonetheless, *Munoz* informs on the District Judge's anticipation of how he would have conducted the balancing analysis later on.

Although not " pre-judg[ing] discovery issues that may arise or deter parties from exercising their rights to seek specific judicial rulings regarding specific discovery issues", the District Judge anticipated that defendant's development of computer capability and facilities in the PRC would likely implicate the SSS. He also recognized the power of the SSL to veer the case off from a fair and full adjudication, stating: "many of the documents that may be subject to assertions of state and archival secrecy **may be relevant—perhaps, highly relevant—**to the issues of this case" [emphasis added]. Id. at *2.

Indeed, this anticipation and concern lurks just below the surface in every *Aérospatiale* balancing analysis: Will the information precluded by the SSL turn out to be critical to a fair adjudication of the liability of the PRC defendant? And if so, shouldn't that concern take center stage in the analysis?

6) In re Grand Jury Investigation of Possible Violations of 18 U.S.C. §1956 and 50 U.S.C. §1705, 381 F.Supp.3d 37 (D.D.C. 2019).

In a criminal matter in which the U.S. government ["gov't"] was looking to prevent North Korea's putative proliferation of weapons of mass destruction, the gov't filed motions to compel testimony and documents from 3 PRC banks. Each bank had been served with a grand jury and/or administrative subpoena relating to the gov't's investigation into money laundering and violations of the U.S. Bank Secrecy Act by a Hong Kong company acting as front for a North Korean state-run entity. The PRC banks asserted the requested discovery of client records had to be produced only under the procedure set forth in the treaty of Mutual Legal Assistance in Criminal Matters [MLAA] and filed motions to preclude. The gov't filed a motion to compel evidence under the subpoenas without going through the MLAA process, which apparently would take quite a long time.

In her *Aérospatiale* balancing analysis, the District Judge stated: "Allowing China to gum up United States' investigations by dictating how the United States can pursue evidence, especially when the two countries'

the advantage of PRC defendants to avoid or minimize their liability in U.S. courts. A tendency to over-preclude Chinese "state secrets" from disclosure can have the result of tipping the balance in favor of advancing the interests of PRC defendants over those of the U.S. by hampering the parties from putting "all relevant cards on the table", thereby moving to a transparent adjudication of liability under the Federal Rules.

Another procedural concern is the uncertainty about the weight accorded to the opinions of ZHP's PRC law experts on how the SSL applies to the 23 documents. Without a direct, *in camera* review of the documents and because of the inherent uncertainty in predicting whether a PRC governmental entity would define any of the disputed documents as a state secret, weighing the reliability and bias of the PRC law expert's analysis is an intellectual and legal black box. With full respect for Ms. Yang's credentials, the Court cannot evidence that her opinion is methodologically reliable.

2.0 Parties Contentions

2.1 ZHP

ZHP's primary legal argument is that the Special Master misapplied 4 of the 5 factors

---

interests are not aligned, is antithetical to sound law enforcement. *[the FBI's declaration] at.* ¶ 83. Furthermore, in some instances the United States **needs access to records without Chinese authorities taking a first pass**. *[the FBI's declaration]* ¶ 84. [emphasis added]. Finally, banks with knowledge that their records might be subject to a federal subpoena, without the shield of the MLAA slow-down process, would have a greater incentive to take care that their customers were not violating United States criminal laws. *[the FBI's declaration]* ¶ 85. These policy rationales instruct against forcing the government to pursue an MLAA." *Id. at 71. …*

"[I]nsofar as the laws at issue here further China's interest in a stable banking system, disclosure to the United States in response to an investigatory subpoena is not a detriment to that interest." *Id*. at 73. … but "the non-enforcement of the subpoenas would undermine the United States national security interests and not undermine any articulated Chinese interest. *Ibid. …* While "the banks have established a basis in Chinese law for the imposition of punishment should any of the banks be compelled to comply with the subpoenas, …such penalties… would be unprecedented." There is no suggestion that the Chinese government would take the counter-intuitive step of imposing heavy penalties against banks in which it has a substantial ownership interest, which "tips ever so slightly toward the banks". *Id*. at 77 …

But, "[o]n balance, international comity is not a reason to refrain from compelling compliance with the subpoenas. **The most important factor, the interests of the relevant countries, could not fall more firmly in favor of enforcement.** [emphasis added]. National security is at stake on one side; on the other, no national interest is compromised "even though the records originated in China, and the banks have acted in good faith, the importance of those factors pale in comparison to the remainder of the balancing analysis." *Ibid.*

Involving very different subject matter than here, all of these cases point to the recognition by U.S. Courts that a well-reasoned balancing of national interests, which is factor 5 in the *Aérospatiale-Wultz* balancing analysis is paramount. *See infra* section 4.2.

enunciated in *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for Southern Dist. of Iowa*, 482 .S. 522, 107 S.Ct. 254, 296 L.Ed.2d 461 (1987), which comprise the determinative balancing test whether non-disclosure of relevant documents withheld under the laws of other countries supplants their required production under the Federal Rules of Civil Procedure ["FRCP"]. Because of this asserted misapplication of relevant law, the Special Master improperly found that 20 of the 23 documents were not governed by the SSL—and specifically, do not relay Chinese state secrets—and therefore wrongly ordered the production of these to plaintiffs.

As a preliminary matter, ZHP does not present legal arguments as to whether the 23 documents at issue are in fact state secrets under Chinese law, but rather relies on the certification of its expert, Ms. Yang, a Chinese lawyer who avers the documents at issue may implicate a Chinese government agency's naming them as state secrets.

ZHP poses an auxiliary argument. Another PRC law, the Data Security Law ["DSL"], in force from 1 September 2021—3 weeks AFTER the issuance of SMO 35—may separately prohibit disclosure of the 23 documents because these documents, having PRC national security interest and located on a server in the PRC, may not be transferred to a foreign court or outside the PRC.

2.2 Plaintiffs

Plaintiffs oppose the motion on principally different grounds than ZHP's. They assert ZHP has not met its burden to provide reliable expert testimony such that the proper PRC government agency would likely find the SSL prohibits disclosure of each document on the Secret Log. Put differently, ZHP has not reliably evidenced that any of these documents contain state secrets as defined in the SSL. Plaintiffs also deduce that since no document on the Secret Log has been shown to contain a state secret, all of them should be disclosed under FRCP 26. Further, the Special Master's balancing analysis of the *Aérospatiale-Wultz* factors (*see infra)* applied proper weight to each factor.

3.0 Legal Standards

3.1 Under *Fed. R. Civ. P. 53 (f)*

Under the FRCP, the court "*may adopt or affirm; modify; wholly or partly reject or*

reverse; or resubmit … with instructions" a Special Master's report and recommendations. *Rule 53(f)(1)*. Review of the Special Master's conclusions of law is *de novo*. *Rule 53(f)(4)*[4]. Where, as here, the parties have not stipulated otherwise, the court also reviews the Special Master's findings of fact de novo. *Rule 53(f)(3)*.

3.2 Under *Aérospatiale-Wultz*

In *Aérospatiale,* the Supreme Court articulated guiding principles as to when U.S. Courts retained jurisdiction to compel discovery of information located outside the U.S. even if a nation's blocking statute forbade the disclosure. The first was that the Hague Convention[5] in no way deprives a District Court of jurisdiction to compel a foreign national party to produce evidence physically located within a Hague Convention signatory nation. 482 U.S. at 539-540. That is, the Hague Convention rules are NOT the exclusive considerations in a U.S. Court's decision to compel. It is important to note here that the Peoples' Republic of China has been a signatory to the Hague Convention since 3 July 1987, before the Supreme Court's guidance in *Aérospatiale*. Thus, the *Aérospatiale* Court considered the obligations of the then-current signatories, which included the PRC, and concluded that the Hague Convention discovery procedure does not supersede the FRCP in a foreign discovery dispute.

Second, neither the Hague Convention nor considerations of comity between nations require U.S. Courts to apply the Convention first before compelling discovery under the FRCP. Courts may equally well consider the FRCP first before Convention principles. *Id.* at 542-544.

Third, the Supreme Court exhorted American courts to "take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state."

---

[4] FRCP 5(f) states:
…
(3) *Reviewing Factual Findings.* The court must decide *de novo* all objections to findings of fact made or recommended by a master, unless the parties, with the court's approval, stipulate that:
(A) the findings will be reviewed for clear error; or
(B) the findings of a master appointed under Rule 53(a)(1)(A) or (C) will be final.
(4) *Reviewing Legal Conclusions.* The court must decide *de novo* all objections to conclusions of law made or recommended by a master.

[5] *Convention on the Taking of Evidence Abroad in Civil or Commercial Matters*, opened for signature 18 March 1970 at the Hague, 23 U.S.T. 2555 ["Hague Convention"].

Id. at 546.

Last, and importantly, although declining to "articulate specific rules to guide this delicate task of adjudication" (*Ibid.*), the Court stated "[t]he nature of the concerns that guide a comity analysis is suggested by the Restatement of Foreign Relations Law of the United States (Revised) § 437(1)(c) (Tent. Draft No. 7, 1986) (approved May 14, 1986) (Restatement)." *Id.* at 544 n.28.

The Restatement lists 5 factors relevant to a balancing analysis. After *Aérospatiale*, district courts have relied on these in deciding whether to compel discovery of foreign documents:

1) the importance to the . . . litigation of the documents or other information requested;
2) the degree of specificity of the request;
3) whether the information originated in the United States;
4) the availability of alternative means of securing the information; and
5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located. *Ibid*.

Courts of the Second Circuit and other jurisdictions have added two more factors to the balancing analysis:
(6) the compliance hardship on the party/witness from whom discovery is sought; and
(7) the good faith of the party resisting discovery. *Wultz v. Bank of China, Ltd.*, 910 F. Supp. 2d 548, 553 (S.D.N.Y. 2012) ["Wultz"].

Currently, District Courts apply all 7 factors to determine whether to compel discovery that is blocked by a foreign statute in what is termed here as an *Aérospatiale-Wultz* balancing analysis.

3.3 *Law of the PRC on Guarding State Secrets* ["State Secret Law" or "SSL"]

The PRC National People's Congress adopted this law on 5 September 5, 1988 and revised it on 29 April 2010. The revision entered in force 1 October 2010. As the PRC government has not issued an official translation into English, the translation used here comes

from Human Rights China.[6]

For this discovery dispute, the pertinent articles include Articles 2 and 9. Article 2 purports to defines state secrets; Article 9 attempts to more specifically enumerate examples of state secrets:

Article 2. State secrets shall be matters that have a ***vital bearing on state security and national interests*** *and, as specified by legal procedure, are entrusted to a limited number of people for a given period of time. ....*

Article 9. The following matters involving state security and national interests, the disclosure of which may harm the country in politics, the economy, defense, foreign affairs, or other such realms, shall be classified as state secrets:

1. Secret matters concerning major policy decisions on state affairs;

2. Secret matters in the building of national defense and in the activities of the armed forces;

3. Secret matters in diplomatic activities and in activities related to foreign countries and those to be kept secret through commitments to foreign countries;

4. Secret matters in national economic and social development;

5. Secret matters concerning science and technology;

6. Secret matters concerning activities for safeguarding state security and the investigation of criminal offenses; and

7. Other matters that are classified as state secrets by the national department for the administration and management of state secret-guarding, [emphasis added]

Especially from Article 9(7), state secrets can encompass an enormous amount of information and are actually defined without a clear boundary. Not only certain kinds of information, but the sources of it, can encompass a state secret. Moreover, the actual determination of what is or not a state secret must be confirmed by national and likely a local agency responsible for state-secret protection.[7] The process of protecting PRC state secrets is

---

[6] Found at https://www.hrichina.org/sites/default/files/PDFs/PressReleases/20101001-StateSecretsLaw-EN.pdf (last accessed 24 November 2021). This is also the translation used by the United Nations, Office of the High Commissioner for Refugees. *See infra* fn. 36.

[7] Articles 5, 10, and 11 of the SSL make the definition of a state secret and its category the function of a state administrative agency as well as of local administrative agencies.

Article 5. The national department for the administration and management of state secret-guarding work shall be responsible for guarding state secrets throughout the country. The local departments for the administration and management of secret-guarding at or above the county level shall be responsible for guarding secrets in their own

done not by reference to the law itself but only by PRC administrative agencies responsible for protecting state secrets. The initial inquiry goes to the State Administration for the Protection of State Secrets (the "SAPSS"), which can basically determine anything to be a state secret. There is no transparency in the agency's determination of what is a state secret.

Article 48 defines SSL violations, which include transferring or transmitting state secrets through electronic means without adopting secret protection measures, such as a check in with the SAPSS.[8] Thus, this article creates the actual blocking prohibition.

Besides the SSL's lack of rigorous definition and knowable process for determining a state secret, its implementing regulations offer little guidance on how a PRC individual/business could determine for itself what is or not a state secret. A PRC business cannot know whether its cross-border transfer of information carries no SSL liability merely by reference to the law itself until it get a determination from the SAPSS and other such agencies

---

administrative areas.

Article 10. State secrets are classified into three categories: "top secret," "highly secret," and "secret."
Secrets classified as "top secret" are the most vital state secrets, the divulgence of which will cause extremely serious harm to state security and national interests;
secrets classified as "highly secret" are important state secrets, the divulgence of which will cause serious harm to state security and national interests; and
secrets classified as "secret" are ordinary state secrets, the divulgence of which will cause harm to state security and national interests.

Article 11. (in part) *The specific scope of state secrets and their classification levels shall be stipulated by the national department for the administration and management of state secret-guarding together with the Ministries of Foreign Affairs, Public Security, and State Security, and other relevant central organs.*
...
Article 20. If organs or units are unclear about or disagree with whether a certain matter is a state secret or its classification level, it shall be determined by the national department for the administration and management of state secret-guarding, or the department for the administration and management of secret-guarding at the level of the province, autonomous region, or directly-administered municipality.

[8] *Article 48. Anyone who violates the provisions of this Law with any [form of] the conduct listed below shall be punished in accordance with the law; if the violation constitutes a crime, the individual shall be prosecuted and held criminally responsible in accordance with the law.*
3. Transferring items bearing state secrets through channels without secret-guarding measures, such as the ordinary postal service and express delivery;
4. Mailing or consigning for shipment abroad items bearing state secrets, or carrying or transferring items bearing state secrets abroad without permission from the relevant departments;
5. Copying, recording, or storing state secrets illegally;
6. Touching on state secrets in private contact or correspondence;
7. Transmitting state secrets through the internet or other public information networks or in wired or wireless communications without having first adopted secret-guarding measures.

of state-secret protection at the provincial or local levels.[9] Adding to the uncertainty, these various agencies may well have conflicting findings as to the nature of a state secret. In addition, Article 29 of the Implementing Regulations 29 state that personnel engaged in "secrets-related business" (again, no definition) must be PRC citizens located within the territory of the PRC.

All of this boils down to: Without definitive approval from one or all of the relevant administrative agencies, non-PRC companies and non-PRC citizens are prohibited from receiving information that contains state secrets, even if unwittingly. Plus, if a non-PRC company has a legitimately-formed subsidiary located in the PRC, non-PRC citizen employees of that subsidiary cannot access state secrets absent approval from the authorities, hence the recommendation to set up appropriate "firewalls" so that only PRC citizens may access the state secret information.[10] Thus, the SSL creates confusion not only for the transfer of legally-requested data in a U.S. litigation, but also for the necessary cross-border transfer of information of PRC businesses operating internationally.

There are 3 types of penalties[11] for violating the SSL with a cross-border transfer of state secret data: Criminal sanctions for intentional or negligent disclosure under "serious" circumstances or for illegally obtaining state secrets, or for unlawfully holding state secrets; Administrative sanctions when disclosure is not deemed serious enough for criminal liability; and Party sanctions for Party members.

---

[9] *See* https://www.hrichina.org/sites/default/files/2014_ssl_implementation_regulations_en_ch.pdf for an unofficial translation of the implementing regulations of the SSL in English (last accessed 24 Nov 2021). Again, there is no official English translation of these regulations issued by the PRC government.

See especially Article 12 of the Regulations , which makes clear the conclusive definition of a state secret is the function of several levels of state-secret guarding administrative organizations.

See also Article 13, which implies an individual entity can submit proposed state secret information to these administrative organizations with their proposed classifications and categories in order to get a determination.

[10] *See* Richard Wigley, *China's State Secrets Law and Compliance Issues for Foreign Companies*, KING & WOODS MALLESON BLOG (2014) https://www.chinalawinsight.com/2014/09/articles/intellectual-property/chinas-state-secrets-law-and-compliance-issues-for-foreign-companies/ (last accessed 24 November 2021).

[11] James Horsley, Draft English Translation, 2014. Implementing Regulations of the Law of the Peoples Republic of China on Guarding State Secrets in force 1 March 2014, Articles 27 to 34, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjF_uLmy9ToAhWdpXIEHc3SBVQQFnoECAUQAQ&url=http%3A%2F%2Fchinalawtranslate.com%2Fwp-content%2Fuploads%2F2014%2F02%2FState-Secrets-Implementing-Regulations-with-Vocab2.pdf&usg=AOvVawodXECQG2S2K01Ff_noraXk (last accessed 8 Dec 2021).

3.4 PRC Data Security Law ["DSL"] and the PRC Personal Information Privacy Law ["PIPL"]

Although ZHP mentions the DSL in its submission, ZHP has not formally briefed either of the two recently enacted PRC laws that also figure as shields against the disclosure of the 23 documents at issue. These are reviewed below to anticipate such briefing .

3.4.1 PRC Data Security Law ["DSL"][12]

DSL Articles 1 and 2[13] speak to its goals and intent regarding safeguarding national security. To that end, the DSL prohibits "data handling activities" within and outside China, which harm national security. Data handling activities include data processing--collection, storage, use, processing, transmission, provision, disclosure--and data management, including archival. In short, data handling is any activity that causes the processing of electronic information stored on a server.

The DSL has no definition of the term national security. There are no Regulations yet. Because of that, extraterritorial enforcement of the DSL will have to arise from treaties or reciprocity agreements between the PRC and other countries. But, more importantly, it can be expected that PRC data handlers will just say no to any request for a cross-border transfer of information they deem even remotely covered by the DSL.[14]

The DSL defines protection of national security to include the prevention of improper

---

[12] Translation: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (last accessed 3 Dec 2021).

[13] ***Article 1:*** *This Law is formulated to standardize data handling activities, ensure data security, promote data development and use, protect the lawful rights and interests of individuals and organizations, and* ***safeguard national sovereignty, security****, and development interests.*

Article 2: *This Law applies to data handling activities and their security regulation within the mainland territory of the People's Republic of China (PRC).* ***When data handling activities outside the mainland territory of the PRC harm the national security****, the public interest, or lawful rights and interests of citizens or organizations of the PRC,* ***legal liability is to be pursued*** *according to the law* [emphasis added].

[14] Xiang Wang, *China's New Data Security Law: What International Companies Need to Know*, ORRICK INSIGHTS, 23 Sep 2021 https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know (last accessed 3 Dec 2021) Multiple PRC governmental authorities are tasked to execute data security matters: 1) the Central National Leadership Organ, which is to issue, overseeing and coordinate national data security strategies and major policies; and 2) local governments and regulatory authorities in their respective regions and industries are to formulate specific catalogues of "important" data. But again, without Regulations, these agencies are likely not up and running yet.

data transfer out of the PRC. The most regulated data are: "Core data", broadly defined as any information that concerns PRC national and economic security, PRC citizens' welfare, and significant public interests. The next most-regulated information is "Important data", which is not as sensitive as core data, but which is undefined, [15] meaning almost any data can be defined as "important".

The DSL imposes data storage and transfer requirements over both the data (core and important) and the data handlers. These include, for example, all IT personnel within a company, or of a cloud company, Internet Service Provider, or of server owners, etc. For example, Critical Information Infrastructure Operators ["CIIOs"] are those data handlers working with informational networks, infrastructure, and natural resources. CIIOs must guarantee data created in the PRC is stored there and must conduct a DSL-mandated security assessment **before** PRC-originated data is sent abroad. For other data handlers, the non-Critical Information Infrastructure Operators ["non-CIIOs"], the DSL will develop additional rules, meaning the national protection measures applied to "important" information is yet unknown.

For both CIIOs and non-CIIOs, the DSL states, qithout approval from PRC authorities, no organizations / individuals in the PRC may transfer data stored there (regardless of where it originated) to any foreign judicial or enforcement authorities. Further, the ambiguous language of the law could enable the government to "retroactively decide that certain information falls under one of the DSL categories, or that a particular use of information violates the law",[16] which emphasizes that this law may encourage PRC defendants and/or PRC data storage handlers to "enforce" this law by simply refusing to transfer requested data.

Even though the DSL names neither the definitive approval process nor the specific PRC approvers, fines for violating it are hefty. Violating organizations face fines of up to 1 million yuan (~$156,854), with additional fines for responsible individuals. Businesses whose violations result in "serious consequences" may face fines of up to 10 million yuan

---

[15] The relevant national, regional and sector authorities are expected to issue catalogs in due course of what counts as "important data."

[16] Yvonne Lau, *Here's what Beijing's sweeping new data rules will mean for companies*, FORTUNE, 1 Sep 2021 https://fortunecom/2021/09/01/china-data-security-law-beijing-management-regulation-internet/ (last accessed 13 Dec 2021).

(~$1,560,854) , the potential suspension of operations, and revocation of the business license.[17]

3.4.2 PRC Personal Information Privacy Law ["PIPL"][18]

This law,[19] which went into effect on 1 Nov 2021, "applies to the activities of handling the personal information of natural persons [located] within the borders of the People's Republic of China".[20] In some respects it mirrors the General Data Protection Regulation ["GPDR"] of the European Union.[21] For example, both PILP and GDPR let individuals access digital and print information held about themselves, seek its correction or deletion, and withdraw consent for their information to be handled by a company.

However, the differences in the PILP are apparent: Article 10 states: *No organization or individual may …engage in personal information handling activities harming national security or*

---

[17] Article 48: Where the provisions of Article 36 of this Law are violated through the provision of data to foreign justice or law enforcement institutions without the approval of managing authorities , relevant departments in charge are to order corrections, may impose a fine of between 100,000 yuan ($15,682.70)and 1,000,000 yuan ($156,854.55) an, and may impose a fine of between 10,000 yuan ($1,568) and 100,000 yuan ($15,682.70) on directly responsible management personnel and other directly responsible personnel; where serious consequences result, a fine of between 1,000,000 yuan($15,682.70) and 5,000,000 yuan ($784,165.17) is to be imposed, and a suspension of relevant operations, a suspension of business for rectification, or the revocation of relevant business permits or licenses may be ordered, and directly responsible management personnel and other directly responsible personnel are to be fined between 50,000 yuan ($7,841.52) and 500,000 yuan ($78,420.12).

[18] This discussion has benefitted from the following sources:
Bingna Guo *et al.*, *China Personal Information Protection Law Will Become Effective Soon*, WHITE & CASE ALERT, 22 Sep 2021 https://www.whitecase.com/publications/alert/china-personal-information-protection-law-will-become-effective-soon (last accessed 15 Dec 2021);
Matt Burgess, *Ignore China's New Data Privacy Law at Your Peril*, WIRED, 5 Nov 2021 https://www.wired.com/story/china-personal-data-law-pipl/ (last accessed 15 Dec 2021);
Paul McKenzie *et al.*, *China's Personal Information Protection Law (PIPL): Key Questions Answered*, MORRISON FOERSTER CLIENT ALERT, 08 Sep 2021;
Michelle Chan *et al.*, *The Gloves are Off! China's Personal Information Protection Law was Passed and will Come into Effect on 1 November 2021*, BIRD & BIRD NEWS CENTER [UK LAW FIRM], 23 Aug 2021 https://www.twobirds.com/en/news/articles/2021/china/chinas-personal-information-protection-law-was-passed (last access 15 Dec 2021).

[19] The translation of the PIPL used here comes from: Rogier Creemers and Graham Webster, DigiChina Project, Stanford University, 7 Sep 2021 https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (last accessed 15 Dec 2021)

[20] Article 3, PIPL.

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, in force 25 May 2018.

the public interest. Article 42 prohibit the access of foreign organizations that harm the national security to personal information of PRC individuals. Thus, the PIPL intertwines the privacy of personal information with the protection of national security. Similar to the DSL, PIPL makes the transfer of personal information stored in the PRC to foreign judicial or law enforcement institutions unlawful, unless approved by the proper PRC regulatory authorities.[22]

The Cyberspace Administration of China (CAC), PRC's internet regulator, which also approves news sources, implements PIPL and is the official national security reviewer of personal information to be transferred out of the PRC. PIPL Article 38 requires companies operating in the PRC to get a national security review by CAC before transferring data out of the PRC. Like the DSL, critical information data handlers (CIIOs) and personal data handlers[23] have to get such a review before they can transfer data out.[24] No cross-border transfer of personal information can occur without some national security review.[25] Even though there are no regulations for the PIPL yet (meaning there are no established protocols for getting a security review, etc.), a company's breach of the PIPL can invoke fines of up to 50 million yuan (~$7.8 million) or 5 percent of its annual revenue as well as civil and administrative penalties. [26]

To summarize for the purposes of this opinion, the PIPL prohibits any transfer of personal information of a PRC individual when that transfer would harm the national security of the PRC or if the information is going to a foreign court.

3.4.3 An *Aérospatiale-Wultz* balancing analysis would apply to DSL and PIPL.

Like the *Munoz* Court, I've anticipated DSL and PIPL may buttress separate arguments

---

[22] Art. 41, PIPL.

[23] Art. 40, PIPL allows Personal Information handlers to adopt alternative processes before transferring data out: to get a certificate from a CAC-approved professional organization that the transferred data are secure; or contract with the overseas recipient using a contract template approved by the CAC.

[24] Art. 58, PIPL.

[25] Of note is the extraordinary extra-territorial application of the PIPL: foreign companies with no operations in the PRC, but engaged in the processing of personal information of persons located in the PRC, are bound by PIPL, and therefore, just like companies operating inside the PRC, must appoint an agent in the PRC for dealing with matters related to the security of personal information.

[26] Chapter VII, PIPL.

for the non-disclosure of these documents and have discussed them to underscore that it is not only the SSL that prohibits cross-border transfer of data classified as having a (vital) national security interest.[27] Moreover, DSL and PIPL restrain not only PRC defendants but also third-party data handlers from complying with Federal Court discovery rules.[28] Third-party data handlers can simply refuse to transfer electronic data—emails, scientific testing and reports, meeting minutes, chemical analyses, etc.—of PRC defendants who may be willing to comply with requests for production in a U.S. litigation. The PRC's ratcheting up of prohibitions against cross-border data transfer can bode badly for PRC defendants in U.S. litigation especially in terms of court-ordered sanctions under Rule 37, if they fail to produce data or deponents because PRC data handlers refuse.

Of interest is the injunction in both DSL and PIPL that information located in the PRC may not be given to U.S. courts. That injunction is inapplicable to these documents or indeed to any information produced in response to an FRCP discovery request. It is not U.S. courts that receive discovery in U.S. litigation, but the parties themselves who exchange information. Consequently, arguments why the DSL and PIPL prohibit cross-border transfer of PRC-located information must rely on the injunction against harming the national security of the PRC, much as has been argued in this motion.

Although no express federal jurisprudence exists yet for these laws, I anticipate that, if used as blocking statutes in U.S. litigation, they would equally call forth the balancing analysis of the *Aérospatiale- Wultz* factors as done below, and very likely would call forth a similar result.

4.0 Discussion

Plaintiffs argue ZHP has not met its burden that the 23 documents convey PRC state secrets as defined by the SSL. ZHP asserts that all 23 documents convey state secrets under

---

[27] Besides these laws, another relatively recent PRC law can generally provide PRC defendants a legal basis to block disclosure in U.S. litigation: the PRC Cybersecurity Law of 2017, which does not appear to be implicated here. Other PRC laws may also serve as similar blocking statutes.

[28] For a discussion as to how the DSL is interrupting not only U.S. litigation but cross-border commerce, *see* Liza Lin and Chun Han Wong, *China Increasingly Obscures True State of Its Economy to Outsiders*, WALL STREET JOURNAL 6 Dec 2021, https://www.wsj.com/articles/china-data-security-law-ships-ports-court-cases-universities-11638803230?mod=Searchresults_pos2&page=1 Access is by subscription only. (last accessed 8 Dec 2021).

the SSL and, because of that, the Special Master wrongly allowed the disclosure of 20 of them by misapplying several of the *Aérospatiale- Wultz* factors.

4.1 Burden of Showing the SSL Prevents Compliance with FRCP

The party invoking a foreign secrecy restriction has the burden not only to assert the basis for its objections with particularity under *Rule 26(b)(5)(A)*[29], but must prove in accordance with *Rule 44.1*[30] that the foreign law applies to the discovery sought, and conflicts with U.S. law.

Plaintiffs assert ZHP has not met its burden to show that the SSL prohibits disclosure of any of the 23 documents at issue. Plaintiffs compare the language of the SSL (translated into English and which translation Ms. Yang, ZHP's Chinese law expert used) with the description of each document—including sender, recipients, and subject matter—to assert that no document at issue falls within the linguistic boundaries of the SSL. Plaintiffs argue Ms. Yang's assertion— that the SSL may well apply to these documents—are from an unreliable expert. To wit, Ms. Yang provided conflicting and consequently unreliable translations of the SSL, which undermines her opinion as to how the SSL applies to the documents. With an unreliable expert, ZHP cannot have met its burden.

In its brief, ZHP does not address directly this contention, but proceeds from the position that SSL may very likely govern the 23 documents and therefore the Special Master's balancing analysis placed too little weight on certain factors because he reached the wrong conclusion and allowed disclosure of 20 of them.

I cannot now rule on whether ZHP has met its burden under *Rule 26(b)(5)(A)*. By this statement, I do not nullify ZHP's responsibility to produce any of the 23 documents at issue. However, without more, such as my *in camera* review of the 23 documents, which ZHP asserts

---

[29] Rule 26(b)(5)(A) states: *When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-preparation material, the party must:*
(i) expressly make the claim; and
(ii) describe the nature of the documents, communications, or tangible things not produced or disclosed--and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.

[30] Rule 44.1 states: *A party who intends to raise an issue about a foreign country's law must give notice by a pleading or other writing. In determining foreign law, the court may consider any relevant material or source, including testimony, whether or not submitted by a party or admissible under the Federal Rules of Evidence. The court's determination must be treated as a ruling on a question of law.*

would violate the SSL, I cannot tender an independent assessment whether the SSL indeed governs these 23 documents and they are likely PRC state secrets.

Simply, at this point, I cannot know without conducting my own independent evaluation. I can neither execute a Daubert-like determination as to the reliability of Ms. Yang's opinions on the reach of the SLL nor resolve with precision the application of the SSL to these documents. There is no confusion that a District Court has the authority to construe the meaning of foreign law and its proper legal application to documents requested to be produced. "Issues of foreign law are questions of law, but in deciding such issues a court may consider any relevant material or source—including testimony—without regard to the Federal Rules of Evidence." *Rule 26.1.*

However, the ambiguous wording of the SSL with its threat of liability coupled with ZHP's concern for that liability have created an impasse that attempts to disarm a district court from making any independent legal review of the application of foreign law. Nevertheless, district courts are not hampered entirely by a foreign law's attempt to block discovery. The Supreme Court and other courts have developed a legal calculus for working through that impasse, which I apply in the Balancing Analysis section below.

4.2 7-Factor *Aérospatiale-Wultz* Balancing Analysis

Given that courts have called this calculus by different terms—a "comity analysis", a "Restatement analysis", etc.—I call the application of the 7 *Aérospatiale-Wultz* factors to the documents at issue a "Balancing Analysis". The term "comity analysis" as used here means the balancing of national interests done in factor 5.

The parties generally agree a Balancing Analysis using the 7 *Aérospatiale-Wultz* factors is the proper legal standard. However, I recognize that performing the Balancing Analysis below implicitly establishes that the documents at issue are governed by the SSL. To the point, I apply the Balancing Analysis below only to resolve the present discovery impasse and expressly reserve judgment as to whether ZHP has in fact met its burden to show these documents indeed relay state secrets under the SSL.

The Supreme Court has found that in a conflict as to the discovery of foreign-initiated evidence, "a court should seek a **reasonable accommodation** that reconciles the central concerns of both sets of laws." *Aérospatiale,* 482 U.S. at 555 [emphasis added]. From the U.S. side, the Federal Rules of Civil Procedure, particularly *Rule 26(b)(1)*, authorize party-

initiated discovery of any evidence relevant to any party's claims or defenses and they also admit court discretion to limit discovery on several grounds, including international comity. *See Id.* at 544. The Supreme Court itself and the Ninth Circuit, however, agree that comity alone to another nation's interest and its foreign law is not dispositive when a discovery dispute arises regarding a foreign law's protection of documents sought in a U.S. court. *See Id.* at 544 & n.29; *Société Internationale pour Participations Industrielles et Commerciales v. Rogers*, 357 U.S. 197, 208 (1958); *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1474–75 (9th Cir. 1992). A court's **reasonable accommodation** arises from its balancing of seven factors to answer what is the greater interest, discovery or preclusion.

From the PRC side, the SSL protects information that responsible government entity(ies) identify as having vital national interest from leaking outside of the PRC. Here the responsible government entities have not so identified and the seeking of this confirmation emerges as a process that is indefinite, non-transparent, and lacking in comity to U.S. courts' need to resolve liability issues for U.S plaintiffs. The indeterminacy of getting a confirmation from PRC government agencies engenders neither patience nor willingness to allow the "gumming up"[31] of this litigation.

The following Balancing Analysis applies generally to 20 of the 23 documents at issue. In SMO 35, the Special Master gave singular consideration to 3 of the documents at issue because various PRC agencies, somewhat akin to the U.S. FDA and its departments, had expressly labelled them confidential reports or communications.[32] For that reason, SMO 35 withheld these 3 documents from discovery. It therefore appeared to the Special Master that these PRC agencies had a greater interest in their non-disclosure than the U.S. had in their disclosure.

It is unclear from the Secret Log description of these 3 documents whether their "confidentiality" equates to "vital national security interest" as used in the SSL. These PRC regulatory agencies are not enumerated in the SSL or its Regulations as having authority to classify their own communications as having "vital national security interest". Nonetheless, if indeed the 3 documents do disclose state secrets, these PRC regulatory agencies bear

[31] *See supra* fn. 6.

[32] SMO 35, Doc. 1482, pg. 16.

ultimate responsibility for protecting them.[33] It is also unclear if these agencies would charge ZHP with liability under the SSL if these 3 documents were disclosed. Because of the greater liability that may attach to the disclosure of these 3 documents, and in reviewing *de novo* the reasons for the Special Master's decision, I concur. These 3 documents are excluded from the Balancing Analysis below, and affirm the Special Master's decision to keep these undisclosed.[34]

The Balancing Analysis below reviews the remaining 20 documents on the Secret Log with these factors:

(1) the importance to the … litigation of the documents or other information requested;

(2) the degree of specificity of the request;

(3) whether the information originated in the United States;

(4) the availability of alternative means of securing the information; and

(5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.

6) the compliance hardship on the party or witness from whom discovery is sought; and

(7) the good faith of the party resisting discovery.

Factor 5: Balancing of National Interests

Not each of these 7 factors carries the same weight. Factor 5, which is itself a balancing within the Balancing Analysis, carries the greatest weight.[35] The underlying key here is the extent to which important interests of the U.S. would be harmed relative to the extent important interests of the PRC would be harmed. For the U.S., the important interest is to

---

[33] Richard Wigley, *China's State Secrets Law and Compliance Issues for Foreign Companies*, KING & WOOD MALLESONS CHINA LAW INSIGHT-INTELLECTUAL PROPERTY, 25 Sep 2014, https://www.chinalawinsight.com/2014/09/articles/intellectual-property/chinas-state-secrets-law-and-compliance-issues-for-foreign-companies/ (last accessed 13 Dec 2021).

[34] SMO 35, Doc. 1482, pg. 16.

[35] *See Aerospatiale*, 482 U.S. at 555-566 [*discussing* the definition, goals, and mechanics of a "comity analysis", which translates into factor 5's balancing of national interests]. *See also supra* fn. 3, demonstrating that U.S. courts have found the so-called "comity analysis" of factor 5 the most important factor.

ensure a fair and transparent legal adjudication of the liability, for any reason, of any of the defendants for the sale in the U.S. of contaminated generic valsartan, irbesartan, and/or losartan.

For the PRC, the important interest is to protect vital national security interests that appear to be protean, defined primarily by a PRC administrative agency's promulgation, and conditioned on specific facts of the moment. Given the very broad flexibility in defining state secrets in the SSL, vital national security interests can get redefined as necessary by the PRC government or administrative agency. Moreover, the SSL expressly gives the PRC governmental agencies the right to retroactively declare information as a state secret.[36] Thus, at this point in the litigation, it is unclear precisely what the PRC's vital national security interests might be with regard to these 20 documents.

The Court makes no assessment about the usefulness to the PRC government of such variability in the definition of (vital) national security interests. However, such variability can serve to justify nondisclosure of any information a PRC governmental agency wants to keep out of U.S. litigation, especially if that prohibition helps to sidestep the liability of large and successful PRC defendants. Moreover, a PRC governmental agency need not affirmatively identify any of these 20 documents as containing vital state secrets, but can let the threat of "big stick" criminal liability motivate PRC defendants to self-limit disclosure of possible state secrets, especially if the information is unfavorable to liability.

Here, where precise and accurately described information in the documents is unknown, balancing factor 5 correctly is critical because this factor buttresses the overall analysis. This requires predicting the most unfavorable result of disclosure and that for nondisclosure, and weighing these against each other. The most unfavorable result for **not disclosing** the 20 requested documents is the absence of a possibly vital piece of information that causes unfair resolution of the litigation, which prejudices plaintiffs **unknowingly**. This is poised against **disclosing** the requested documents and thereby revealing information of vital national security interest to the PRC, which triggers civil and/or criminal liability for ZHP.

From all sources considered the most unfavorable result of disclosure does not rise to

---

[36]United Nations, Office of the High Commissioner on Human Rights ["UNHCHR"], UN Treaties Database, Shared SharePoint Database, ANNEX A – Outline of States Secrets Framework in the People's Republic of China, No. INT_CRC_NGO_CHN_13772_E 19 June 2014 at https://tbinternet.ohchr.org/Treaties/CRC/Shared%20Documents/CHN/INT_CRC_NGO_CHN_13772_E.pdf (last accessed 14 Dec 2021). Note the UNHCHR relies on the English translation of the SSL cited *supra*, fn. 6.

the extent of injury caused by the most unfavorable result of non-disclosure. These sources include: Ms. Yang's declaration the documents may implicate the SSL; plaintiffs' arguments that none of these implicate the SSL; external sources casting doubt on PRC's likelihood of meting out a harsh liability to a successful PRC enterprise;[37] and Mr. Chen's, ZHP's CEO, membership in the Communist Party, which may modulate ZHP's overall liability.

I therefore find that factor 5 tips heavily in favor U.S. interests and disclosure of the 20 documents.

Factor 1: Importance of the Requested Information to the Litigation

Factor 1 actually flows from Factor 5 in that it provides more specific information to tip factor 5 one way or another. In their brief (Doc.1570: 19-21), plaintiffs do not assert a specific, qualitative measure of the importance of the these documents to the litigation. The Special Master noted plaintiffs did argue these documents are important because they involve particular communications that lie at the heart of the litigation. Doc. 1482:12-13.

ZHP cited the same case the Special Master cited, *In re Activision Blizzard*, 86 A.3d 531, 544 (Del. Ch. 2014), to argue factor 1 requires that the requested documents exhibit relevance to the litigation that goes beyond "merely relevant" to the level of "directly relevant". *Strauss v. Credit Lyonnais*, S.A. 249 F.R.D. 429, 440 (E.D.N.Y. 2008) discusses more fully the kind of relevance that satisfies factor 1:

> "Because the scope of civil discovery in the United States is broader than that of many foreign jurisdictions, some courts have applied a more stringent test of relevancy when applying the Federal Rules to foreign discovery. *See Aerospatiale,* 482 U.S. at 542, 546, 107 S.Ct. 2542 (*noting* that the requested documents were "vital" to the litigation, and advising U.S. courts that "[w]hen it is necessary to seek evidence abroad ... the district court must supervise pretrial proceedings particularly closely to prevent discovery abuses"); ... *but see Compagnie Francaise d'Assurance Pour le Commerce Exterieur v. Phillips Petroleum Co.*, 105 F.R.D. 16, 32 n. 8 (S.D.N.Y.1984) ("In ordering production of

[37] *See* Fu Hualing, *The Secrets about State Secrets: the Burden of Over-Classification*, 14 JOURNAL OF COMPARATIVE LAW 249, 264 (2019).

these documents, this Court does not need to find, nor can it find at this point, that the requested documents are 'vital'...."); *Graco, Inc. v. Kremlin, Inc.*, 101 F.R.D. 503, 515 (N.D.Ill.1984) (noting that *Aerospatiale* indicated that the requested discovery should be "vital," but declining to articulate a standard)".

ZHP claims the requested documents are not "vital" primarily because these discuss events and communications related to the Chinese, not the U.S., market. ZHP argues that communications with PRC regulatory agencies charged with the safety or perception of safety of ZHP-manufactured drugs in and by the Chinese market can have nothing to do with this litigation concerning the U.S. market. ZHP also asserts that neither does the request from the PRC government about how to manage untrue and misleading information on the Internet regarding drugs sold in the Chinese market.

ZHP's claim, however, goes to the cultural context of the communications not to their content or consequences. ZHP also argues these documents discuss other than a root-cause investigation into valsartan impurities; but, that argument does not speak directly to whether the subject matter of these may be "vital" to the litigation in another way. Particularly curious is that ZHP's own summary of the documents (Doc. 1551-1, Exhibit B) discloses topics which, if conveyed by the FDA, the European Medical Agency, or other national drug testing agencies, would be considered highly relevant for their fact-finding about contaminant / contamination details. To the point, ZHP lists documents that purportedly discuss testing the drug products for sale; on-site inspection of ZHP; summaries from experts of various PRC drug evaluators of drug safety; detection of NDEA impurity in irbesartan; reports to local municipal governments about misleading information from public media about the valsartan contamination; a report from the local commerce bureau as to why the import ban of ZHP's products occurred. With the benefit of hindsight and the history of previous reports from the FDA and the EMA, these documents may appear not particularly relevant now. But, in looking back to the early days when contamination was first discovered and when these documents were prepared or meetings held, these documents may have concerned important information, regardless of the market being discussed.

As stated above, Factor 1 supplements the comity analysis of Factor 5 by providing more specificity. The Court's research found that relevant caselaw does not define a standard of what documents constitute "directly relevant" or "vital to a litigation" such that the 20

disputed documents fall neatly into a category of favoring disclosure or not. That is, the standard for relevance under factor 1 is not as black and white as argued. Documents need not be "vital" to be important to the litigation. The 20 documents at issue here and summarized in Doc. 1551-1, Exhibit B display context (if not actual content) that concerns the how, and possibly the why, of the valsartan API contamination, regardless of where the finished drugs were sold. Given this supplementation to Factor 5, I find the summary in ZHPs Exhibit B favors disclosure as the 20 documents appear important to the litigation.

Factor 2: The Degree of the Specificity of the Request

The discovery of the 20 documents at interest arise from plaintiffs' requests for production ["RFP"]. More than two years ago, the parties themselves, aided by Magistrate Judge Schneider, negotiated extensively the RFPs both in terms of their language and specificity. No good reason has been advanced to consider the RFPs are over-specific. This factor does not advance the prohibition of the documents and accordingly, favors disclosure.

Factor 3: Whether the Information Originated in the United States

That the information originated in China is why ZHP declares the SSL may govern the disclosure of the 23 documents at issue. Clearly, this factor favors non-disclosure.

Factor 4: The Availability of Alternative Means of Securing the Information

As stated above, ZHP argues several of the documents at issue are irrelevant because they concern communications about the Chinese market. Of those documents that do discuss other topics, ZHP states the information contained therein is available from other sources, largely reports given to, or gotten from, drug regulatory agencies in other jurisdictions, like the FDA or the European Medical Agency, etc. ZHP argues specifically that one document, ZHP02608729, would be cumulative to information ZHP has already provided to the FDA and is therefore alternatively discoverable. ZHP also argues generally that the 3.5 million pages it has already produced includes communications with the FDA and other such agencies as well as its own internal and external communications regarding the root analysis of the contamination. The implication is there can be no need to secure the information in the 20 documents at issue as that has most likely been provided already.

While appreciating ZHP's argument that quantity of production likely generates redundancy in disclosure, I do not endorse it. The "quantity" argument presents a logical sleight of hand. On the one hand, ZHP argues these documents, as possibly containing state secrets, are therefore undiscoverable under the SSL. On the other hand, however, the tremendous amount of information ZHP has already disclosed likely makes these documents cumulative. The fundamental question is, How can it be known if these 20 undisclosed documents do indeed contain state secret information that has already been disclosed by other, not PRC-originated documents? It's speculation as to whether any of the 20 documents at issue, even ZHP02608729, can be labelled cumulative. There's been no specific showing that:

The Secret Log description of any of the 20 documents expands upon already disclosed information; none of these 20 provides necessary bedrock information; or

each of these is cumulative of other documents already produced.

Absent good reason to find these 20 documents cumulative or not, I find this factor favors neither disclosure nor non-disclosure.

Factor 6: The Compliance Hardship on the Party / Witness from Whom Discovery is Sought

The next two factors were not included in the original Foreign Relations Restatement list used by the *Aerospatiale* Court, but added later by Second Circuit[38] courts to modulate the very great weight of factor 5. To reiterate, not all factors in the balancing analysis pose equal weight, which means the balancing analysis is not simply a tally of disclosure vs non-disclosure factors to arrive at a "score" and therefore a decision.

If the SAPSS in the PRC decided definitively that these 23 documents do contain state secrets, there is no question that ZHP may face civil and criminal liability under the SSL, and therefore no question that this factor favors non-disclosure.

Two considerations nonetheless modulate the weight of this factor. First, at this point, it is only a possibility that ZHP would be found liable of a violation of the SSL if these documents were disclosed. In separate research, I have found few reported PRC cases that

[38] *Wultz*, 910 F.Supp.2d at 553; *Strauss*, 249 F.R.D. at 438–39 [*citing Minpeco S.A. v. Conticommodity Servs., Inc.*, 116 F.R.D. 517, 523 (S.D.N.Y.1987)].

have meted out liability against PRC enterprises for disclosing state secrets. Granted, this paucity may be because state secret cases are conducted in secret in the PRC.[39] Almost all information readily available about this topic relates to the *Rio Tinto* case resolved before the current revision of the SSL (and therefore not discussed here) or to cases against PRC citizens in Hong Kong who have expressed unfavorable views against the PRC government.[40]

But, these cases did not have the context of this situation: where ZHP is a very large pharmaceutical company adding to the PRC economy.[41] Some pundits believe the SSL is a sword of Damocles to keep international business in line but infrequently wielded if ever against a titan of the PRC economy. Both the unproven nature of the liability and the PRC's apparent reluctance to carry out such liability against a successful PRC enterprise mitigate the weight accorded this factor.

The second consideration is that ZHP and the plaintiffs together can minimize disclosure of the information in the 20 documents at issue. Effective means include confidentiality agreements, court-ordered sealing protections, and cooperative efforts to reduce transmission among the parties before trial. Such cooperative efforts have been adopted in similar situations involving blocking statutes.[42] Further, if the parties resolve a settlement before any of the documents are used at trial, these will not enter the public record. Thus, by taking active measures to avoid public disclosure, the parties can together confirm ZHP's efforts to navigate the legal (and possibly political) dilemma in which it now finds itself, which may lessen its exposure under the SSL, and correspondingly lessens the weight of this factor.

---

[39] Sigrid Jernudd, *China, State Secrets, and the Case of Xue Feng: the Implication for International Trade*, 12(1) CHICAGO JOURNAL OF INTERNATIONAL LAW, Article 12, pg. 330 (2011), available at https://chicagounbound.uchicago.edu/cjil/vol12/iss1/12?utm_source=chicagounbound.uchicago.edu%2Fcjil%2Fvol12%2Fiss1%2F12&utm_medium=PDF&utm_campaign=PDFCoverPages (last accessed 14 Dec 21).

[40] The Congressional- Executive Commission on China (independent agency of the U.S. government that monitors human rights violations and the rule of law development in the PRC) has reported on the prosecution of individuals for national security violations here, https://www.cecc.gov/silencing-critics-by-exploiting-national-security-and-state-secrets-laws (last accessed 14 Dec 2021). The U.S. government's reporting on such cases of SSL liability being brought against PRC dissidents may have its own political implications.

Also, *see infra* fn. 43 for a brief discussion on the SEC audit cases.

[41] https://www.wsj.com/market-data/quotes/CN/XSHG/600521/company-people, Access is by subscription only. (last accessed 2 December 2021).

[42] *See In re Activision Blizzard*, 86 A.3d 531 (Del. Ch. 2014).

Factor 7: The Good Faith of the Party Resisting Discovery.

Although plaintiffs argue that ZHP has not exercised good faith during the months of ferreting out what documents should or not be produced under the SSL, ZHP's efforts do not show bad faith. Specifically, that ZHP started out with a very large number of documents withheld under the SSL and then whittled that number sequentially indicates not bad faith but rather confusion or lack of clarity about the SSL, which as discussed earlier is admittedly vague and of little legal help. I recognize ZHP's efforts to engage a Chinese law expert as well as the expert's own need to get an improved English translation of the SSL, which may have affected her earlier opinion. I also note ZHP's request to the PRC SSL authority to get, as the SSL requires, the determination as to whether the SSL applies here.

Although favoring non-disclosure, the factor by no means outweighs or comes close to the determinative power of factor 5. This is so because, to observe the obvious, the parties in any federal litigation are always called upon to act in their "best" good faith in cooperating with, and applying their advocacy before, the Court. Thus, this factor looks at the behavior a party should do, not at exceptional behavior. And, ZHP has met that behavioral standard.

5.0 CONCLUSION

A simple tally of these factors favors disclosure:

Factor 5 favors: disclosure

Factor 1 favors: disclosure

Factor 2 favors: disclosure

Factor 3 favors: disclosure

Factor 4 favors: neither, neutral

Factor 6 favors: non-disclosure

Factor 7 favors: non-disclosure

However, as mentioned above, rather than be a simple tally of the factors, a Balancing Analysis should embrace much of the background and circumstances of the discovery dispute. I acknowledge that ZHP perceives disclosure of any of these documents risks its liability under the SSL in terms of money fines and criminal sanctions. Further, by disclosing these

documents, ZHP may risk liability of violating 2 other Chinese laws relating to data security and the protection of personal information. Although appreciating ZHP's dilemma, I cannot subordinate the legitimate interests of U.S. plaintiffs in determining civil liability and possibly money damages because of uncertain-at-this-point-but-perceived liability under the SSL.

In the "big picture" balancing of which national interests weigh more, I found two points important. First, none of the SSL, its regulations, the DSL, or PPIL defines with particularity a **vital** or otherwise national security interest. This inherent doubt as to the definition of a state secret or "national security interest" militates automatically for non-disclosure of any information created or stored in the PRC. Put differently, a vague definition pushes a PRC defendant to draw a wide boundary around those documents that may fit the definition and especially encourages non-disclosure of incriminating information.

Second, the lack of transparency and comity by which a PRC governmental entity determines how and whether a document contains information of vital national security interest leads to the inevitable questions as to that determination's timeliness and fairness. Specifically, it's unclear from the SSL whether multiple governmental entities at different levels of government, national, provincial, municipal should decide a document contains a state secret, and how and whether a PRC defendant can actually get a definitive answer. Moreover, the process of getting even an initial answer seems generally to take longer than the typical U.S. litigation discovery period of over two years.[43] Thus, from the perspective of U.S. Courts and U.S. plaintiffs, checking-in with a PRC governmental agency as to vital national security interests has the consequence of gumming up U.S. litigation, without a strong good cause.

In sum, the legal uncertainty as to what is a PRC state secret and in getting a definitive, final confirmation creates a blocking statute that is a textbook example of how to limit / avoid discovery of relevant information that may evidence a PRC defendant's liability to U.S. plaintiffs. An additional consideration is, although the PRC laws do enumerate both fines and criminal liability, there is very little direct evidence that shows a PRC government entity actually levying penalties against successful and behemoth PRC defendants engaged in U.S. products liability litigation.

---

[43] David Moncure, The Conflict Between United States Discovery Rules and the Laws of China: The Risks Have Become Realities, 16 SEDONA CONFERENCE JOURNAL 283, 302-306 (2015).

From the perspective of a PRC defendant engaged in U.S. litigation, it would be unskillful not to invoke the SSL and other PRC data security laws even if there were no serious threat of potential liability being meted out for their violation. From the perspective of U.S. plaintiffs, a skillful litigation tactic of a PRC defendant cannot outweigh the possible injury of those in the U.S. market who took contaminated medicine trusting it would keep them healthy.

In looking at the likely effect these PRC laws do and will have on the U.S. market, I find this a most important consideration. Even though between a" legal rock and hard place", PRC defendants cannot enter the U.S. market expecting a possible shield from unfavorable discovery by PRC blocking statutes. As one judge's decision has implied, if you don't like the rules, then stop doing business in the U.S.[44]

Any expectation that a PRC law will successfully shield discovery in a U.S. litigation needs a tempering of realism. That is, PRC defendants must know from the outset they risk serious consequences if and when they fail to obey a U.S. court's order to compel discovery. These consequences arise from the clearly enumerated authority under Rule 37,[45] which U.S.

---

[44] *Id.*, at 308, *discussing* SEC Administrative Law Judge Elliot's decision in a consolidated SEC enforcement action against several PRC companies whose audit papers (in the PRC) were requested by the SEC. The PRC companies refused citing the PRC SSL. Nonetheless, Judge Elliot found the audit firms, many of which were registered in the U.S. and which held the papers in their Chinese subsidiaries, liable for non-compliance with the Sarbanes-Oxley Act. In the end, four of the five audit firms for the PRC companies agreed to a settlement with the SEC that involved a $500,000 fine against each of the settling firms. There was some working through the SSL violations with Chinese regulators, but not all PRC liability resolved. S*ee id., at 284-291.*

See the decision at *BDO China Dahua CPA Co. Ltd.*, Initial Decision Release No. 553, 2014 SEC LEXIS 234 (Public) (22 January 2014).

[45] In relevant part, Rule 37 states:

FAILURE TO MAKE DISCLOSURES OR TO COOPERATE IN DISCOVERY; SANCTIONS

. . .

(b) Failure to Comply with a Court Order.

. . .

(2) Sanctions Sought in the District Where the Action Is Pending.

(A) For Not Obeying a Discovery Order. *If a party or a party's officer, director, or managing agent—or a witness designated under Rule 30(b)(6) or 31(a)(4)—fails to obey an order to provide or permit discovery, including an order under Rule 26(f), 35, or 37(a), the court where the action is pending may issue further just orders. They may include the following:*

(i) directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;

(ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence;

(iii) striking pleadings in whole or in part;

courts wield as needed.

An example of a court imposing such a tempering realism is found *In re Activision Blizzard, Inc.*, 486 A.3d 531, 552 (De. Ch. Ct. 2014). There, the court required French defendants to make a good faith effort to obtain promptly the assistance of the appropriate French authority in deciding the disclosable nature of documents at issue. This good faith effort is similar to what I see ZHP has done. However, the *Activision* court's patience was not infinite in that the French defendants were given a deadline by which the blocked French documents had to be produced, with or without the French authority assistance. The court stated:

> *"If [document] production has not been authorized [by the French authority] by March 31, 2014, when substantial completion of document production is due, then the [French] Defendants shall produce on that date the documents called for by the plaintiff's discovery requests or face the prospect of sanctions in this court. In considering sanctions, the court will be guided by the factors cited in Section 442 of the Restatement [Third of the Foreign Relations Law] and will take into account the recommendation in Section 442(2)(c)[46] of the Restatement that the*

(iv) staying further proceedings until the order is obeyed;
(v) dismissing the action or proceeding in whole or in part;
(vi) rendering a default judgment against the disobedient party; or
(vii) treating as contempt of court the failure to obey any order except an order to submit to a physical or mental examination.

[46] Restatement (Third) §442(2) of the Foreign Relations Law states:

If disclosure of information located outside the United States is prohibited by a law, regulation, or order of a court or other authority of the state in which the information or prospective witness is located, or of the state of which a prospective witness is a national,

(a) a court or agency in the United States may require the person to whom the order is directed to make a good faith effort to secure permission from the foreign authorities to make the information available;

(b) a court or agency should not ordinarily impose sanctions of contempt, dismissal, or default on a party that has failed to comply with the order for production, except in cases of deliberate concealment or removal of information or of failure to make a good faith effort in accordance with paragraph (a);

(c) a court or agency may, in appropriate cases, make findings of fact adverse to a party that has failed to comply with the order for production, even if that party has made a good faith effort to secure permission from the foreign authorities to make the information available and that effort has been unsuccessful.
[emphasis added]

appropriate sanctions involve making 'findings of fact adverse to a party that has failed to comply with the order for production, even if that party has made a good faith effort to secure permission from the foreign authorities to make the information available and that effort has been unsuccessful.' Restatement § 442(2)(c)."

Importantly, the non-compliance of a Court Order risks the imposition of Rule 37 sanctions. To temper the harsh reality that ZHP finds itself in, the parties' utmost cooperation is required to prevent public disclosure of these documents at this point in the litigation.

Accordingly, **the COURT:**

DENIES ZHP's motion to vacate SMO 35; and

AFFIRMS SMO 35 in its entirety; **and**

ORDERS:

Plaintiffs' Motion To Compel (Doc. 1231) is **GRANTED IN PART AND DENIED IN PART; and FURTHER ORDERS:**

by the next Case Management Conference ["CMC"] in this MDL scheduled to occur on 5 Jan 2022, ZHP shall produce all documents that are the subject of Plaintiffs' Motion to Compel, along with all documents listed as duplicates of these documents on its State Secrets Review Log of documents withheld as Chinese state secrets, with the exception of the following three documents and any duplicates of the following three documents: ZHP0255672, ZHP02622051, and ZHP02622054;

and FURTHER ORDERS

the 20 documents affirmed here as discoverable shall be disclosed to plaintiffs in the same format (i.e., redacted or original) as ordered in SMO 35;

and **only to select** members of plaintiffs' executive committee ["PEC"] having an immediate need to know, as determined by Plaintiffs' Lead Counsel (*See Case Management Order No.* 6, Doc. 96);

the PEC shall create and maintain a Disclosure Log from the date of the next CMC, which in real time records and archives disclosure details, that is, which attorneys of the PEC have been given access; what document(s); and the date of disclosure;

PEC attorneys who have been given access to any document(s) on the State Secret Review Log shall adopt best practices to maintain the secrecy and confidentiality of the

document(s);

no member of the PEC nor other of plaintiffs' attorneys shall distribute, disclose, or recite any, or any portion, of these 20 disclosed documents to other plaintiffs' attorneys who are not members of the PEC without first making a motion for such disclosure to the Special Master for exceptional cause; and

if the Special Master allows disclosure to other plaintiffs' attorneys, then the PEC shall update in real time the Disclosure Log.

Dated: 18 Dec 2021

s/ Robert B. Kugler
Robert B. Kugler
United States District Judge