UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 82 ● Fall 2020

NOTES

THE FORTIFICATION OF THE GREAT FIREWALL AND ITS EFFECT ON E-DISCOVERY DISPUTES IN U.S. COURTS

Keeton Christian

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

NOTES

THE FORTIFICATION OF THE GREAT FIREWALL AND ITS EFFECT ON E-DISCOVERY DISPUTES IN U.S. COURTS

Keeton Christian*

Table of Contents

* J.D., 2020, University of Pittsburgh School of Law; M.Ed., 2010, University of Tennessee at Chattanooga; B.A., 2009, University of Tennessee at Chattanooga.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

INTRODUCTION

In the realm of cross-border e-discovery, United States courts must balance the American ideal that expansive discovery leads to just outcomes,[1] their robust power to compel production of electronically stored information ("ESI") stored abroad,[2] and their duty to consider foreign laws blocking production of ESI stored within foreign territories.[3] Recently, the predicament has become increasingly more fraught with the proliferation of potentially discoverable ESI[4] and the concurrent promulgation of stricter data protection laws and regulations in foreign jurisdictions.[5]

The newly enacted Personal Information Security Specification[6] ("Specification") is one step in China's overhaul of its data privacy laws and regulations that began with the passage of the Cybersecurity Law of the People's

[1] "We agree, of course, that the . . . discovery rules are to be accorded a broad and liberal treatment. No longer can the time-honored cry of 'fishing expedition' serve to preclude a party from inquiring into the facts underlying his opponent's case. Mutual knowledge of all the relevant facts gathered by both parties is essential to proper litigation." Hickman v. Taylor, 329 U.S. 495, 507 (1947).

[2] The Supreme Court of the United States explained that it would undermine the Federal Rules of Civil Procedure to hold that a party lacks "control" of a document simply because the litigant could face punishment under foreign laws where the document was located if the litigant produced the document in pretrial discovery. Société Internationale Pour Participations Industrielles et Commerciales v. Rogers, 357 U.S. 197, 205 (1958). *See* Joseph Perkovich, *U.S. Court Control of International Discovery Practice*, *in* EDISCOVERY FOR CORPORATE COUNSEL § 21:2 (2019).

[3] "American courts, in supervising pretrial proceedings, should exercise special vigilance to protect foreign litigants from the danger that unnecessary, or unduly burdensome, discovery may place them in a disadvantageous position . . . . [W]e have long recognized the demands of comity in suits involving foreign states, either as parties or as sovereigns with a coordinate interest in the litigation." Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 546 (1987).

[4] *See Data Never Sleeps 5.0*, DOMO, https://web-assets.domo.com/blog/wp-content/uploads/2017/07/17_domo_data-never-sleeps-5-01.png (last visited Nov. 15, 2020), for a visual representation of the vast amounts of data that is created every minute of the day.

[5] "[General Data Protection Regulation] wasn't the beginning and it certainly won't be the end. Strict data privacy legislation is appearing in more and more economies across the globe." Dan Simmons, *6 Countries with GDPR-like Data Privacy Laws*, COMFORTE INSIGHTS (Jan. 17, 2019), https://insights.comforte.com/6-countries-with-gdpr-like-data-privacy-laws. *See* M. James Daley, Jason Priebe & Patrick Zeller, *The Impact of Emerging Asia-Pacific Data Protection and Data Residency Requirements on Transnational Information Governance and Cross-Border Discovery*, 16 SEDONA CONF. J. 201, 249 (2015), for an overview of data privacy laws in Asian countries as of 2015.

[6] Mingli Shi et al., *Translation: China's Personal Information Security Specification*, NEW AMERICA (Feb. 8, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/ [hereinafter *Specification*].

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

Republic of China ("Cybersecurity Law") in 2016.[7] The new data privacy legal paradigm in China has the potential to further complicate the already complex landscape[8] of e-discovery in U.S. courts involving ESI stored in China.

With the interconnectedness of the U.S. and Chinese economies,[9] the increasing reliance on electronic data,[10] and Chinese data localization requirements,[11] litigants increasingly find themselves in a jam when ESI stored in China is discoverable under the Federal Rules of Civil Procedure ("FRCP"), but Chinese data privacy laws forbid transfer of the data and potentially punish data controllers who use the data in opposition to the laws.[12] Before China overhauled its personal data privacy laws, U.S. courts tended to order production of the ESI, invoking the power of the FRCP to compel production of the data.[13]

This Note explores how the new data privacy legal paradigm in China may impact discovery disputes in U.S. courts involving ESI stored in China. Part I discusses the current legal framework on which U.S. courts rely to resolve discovery disputes involving foreign-stored ESI. It examines how U.S. courts decided and analyzed discovery disputes involving ESI stored in China preceding the issuance of the Specification and Cybersecurity Law. Part II discusses the new personal data privacy legal paradigm in China and its effect on cross-border discovery. It argues that the new law and guidelines will likely have minimal effect on U.S. courts' analysis of e-discovery disputes involving data stored in China. Part III argues that altering U.S. courts' analysis to favor increased reliance on the Hague Evidence

[7] Rogier Creemers et al., *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, NEW AMERICA (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ [hereinafter *Cybersecurity Law*].

[8] *See generally* Rob Hellewell & Michelle Mattei, *Behind the Great Firewall of eDiscovery in Asia*, ASS'N OF CORP. COUNSEL 28, 32 (Sept. 1, 2014), https://www.acc.com/sites/default/files/resources/vl/public/ACCDocketArticle/1375727_1.pdf.

[9] *Fact Sheet: U.S.-China Economic Relations*, THE WHITE HOUSE (Sept. 04, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/09/04/fact-sheet-us-china-economic-relations.

[10] "The explosive growth in the reliance on electronic data integrated in webs of geographically dispersed communication networks has increased the volume and variation of material beyond U.S. borders yet susceptible to the scope of discovery in U.S. litigation." Perkovich, *supra* note 2.

[11] *See infra* Part I.

[12] *See infra* Part I.

[13] *See infra* Section I.C.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

Convention would likely not result in just and efficient discovery outcomes in line with American ideals favoring vast pretrial discovery.

I. CROSS-BORDER E-DISCOVERY LEGAL FRAMEWORK

During the discovery phase of litigation in U.S. courts, litigants exchange evidence and the names of potential witnesses they may present at trial.[14] The Federal Rules of Civil Procedure govern the process.[15] U.S. federal courts' commitment to broad discovery[16] distinguishes the U.S. pretrial process from other jurisdictions.[17] The vast, party-driven American discovery procedure varies greatly from the evidence disclosure process that judges primarily spearhead in civil law systems like China's.[18]

The vastness of discovery in U.S. courts reaches beyond its own borders. U.S. courts have the power to compel parties to produce ESI stored in foreign jurisdictions, even when foreign data privacy laws deem a cross-border transfer illegal.[19] This section delineates the tension between the U.S. preference for broad

---

[14] FED. R. CIV. P. 26; *see also How Courts Work: Discovery*, ABA (Sept. 9, 2019), https://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/discovery/.

[15] FED. R. CIV. P. 26(a)(1); FED. R. CIV. P. 27–32; FED. R. CIV. P. 33; FED. R. CIV. P. 34; FED. R. CIV. P. 36; FED. R. CIV. P. 26(a)(2); *see generally* Practical Law Litigation, E-DISCOVERY GLOSSARY, Westlaw (database updated 2020).

[16] *Supra* note 1 and accompanying text (quoting Hickman v. Taylor, 329 U.S. 495, 507 (1947)); *see also* Plata v. Brown, 754 F.3d 1070, 1078 (9th Cir. 2014) (explaining that "mutual knowledge of all relevant facts" is a "fundamental principle" of proper litigation).

[17] Perkovich, *supra* note 2. Though the U.S. model of pretrial discovery is the most broad, English courts may order a party to disclose specific documents and permit the requesting party to inspect the documents. *See* CPR, Rule 31.2; CPR, Rule 31.3. Distinctly, litigants do not have mechanisms for compelling parties or witnesses to produce evidence directly to them in civil law jurisdictions. Instead the litigants produce evidence to the courts. Lukas Holub, *Discovery Abroad: An Overview of European Blocking Statutes and the Hague Convention on the Taking of Evidence Outside the U.S.*, NITA (Apr. 4, 2019), https://www.nita.org/blogs/discovery-abroad-an-overview-of-european-blocking-statutes-and-the-hague-convention-on-the-taking-of-evidence-outside-the-uspart-one-of-two#_ftn16.

[18] Judge Elizabeth Fahey & Judge Zhirong Tao, *The Pretrial Discovery Process in Civil Cases: A Comparison of Evidence Discovery Between China and the United States*, 37 B.C. INT'L & COMP. L. REV. 281, 283–88 (2014) [hereinafter *China and the United States*].

[19] The United States District Court for the Southern District of New York ordered the Bank of China to produce documents despite the court's finding that the production of the documents in the U.S. would violate Chinese state secret laws. Wultz v. Bank of China Ltd., 942 F. Supp. 2d 452, 466, 473 (S.D.N.Y. 2013); *see also* Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 546 (1987).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

discovery and foreign nations' interests in protecting the data that flows from within their borders, as well as how that conflict unfolds in U.S. courts. Section A discusses the underlying conflict and how nations have attempted to remedy it. Section B discusses how U.S. courts analyze the conflict in transnational discovery disputes. Section C discusses disputes involving ESI stored in China that preceded the recent overhaul of privacy laws in China.

A. Vast U.S. Discovery vs. Protective Data Privacy Laws

1. Comparing Evidence Exchange Processes in the United States and Civil Law Jurisdictions

Conflicts arise when litigants engaged in U.S. discovery seek ESI stored in countries with comparatively broader data protections and narrower pretrial evidence exchange processes. Discordant legal paradigms regarding privacy and evidence disclosure underlie the clash between U.S. courts' expansive discovery and foreign jurisdictions' restrictive data protection laws.[20]

The U.S. system of pretrial discovery relies on the fundamental concept that active involvement of individual litigants "is most likely to achieve fair administration of justice."[21] In contrast, in civil law countries, the court, rather than individual litigants, manages the evidence exchange process.[22] Further distinguishing the processes from discovery in U.S., in civil law jurisdictions, including China,[23] litigants are required to disclose less evidence throughout the litigation process, and are required to disclose very little evidence during the pretrial discovery.[24] The authors of *The Sedona Conference Practical in-House Approaches for Cross-Border Discovery & Data Protection* explain that civil law practitioners assume that the judiciary is best positioned to direct evidence disclosures to protect the privacy of individuals that could be potentially compromised in a U.S.-style

[20] ABA HOUSE OF DELEGATES, RESOLUTION 103, at 4 (Feb. 6, 2012).

[21] The Sedona Conference, *The Sedona Conference Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 17 SEDONA CONF. J. 397, 405 (2016) [hereinafter *Sedona Discovery & Data Protection*].

[22] *Id.*; *see infra* Section I.A.3.

[23] *See infra* Section I.A.3.

[24] *Id.* For example, in Germany litigants must appeal to the court when seeking production of documents. *Sedona Discovery & Data Protection*, *supra* note 21, at 406. If the court grants the request for the document, the opposing party must only produce documents beneficial to its case. *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

litigant-driven process.[25] While the U.S. judiciary oversees an evidence exchange process in which most evidence is requested and produced to individual litigants before the trial process begins, civil law jurisdictions, including China, entrust the judiciary to actively manage the process.[26] Additionally, civil law jurisdictions heavily restrict what evidence disclosures individual litigants receive and are required to produce—protecting the privacy rights of individual litigants.[27]

2. U.S. and China: Inverse Legal Privacy Paradigms

The difference between the discovery process in the U.S. and the civil law-based evidence disclosure process utilized in China illustrates the inverse legal privacy paradigms in the two countries. U.S. courts' broad pretrial discovery process relies on the active involvement of individuals and the "mutual knowledge of all relevant facts"[28] to achieve justice. The Chinese civil law-based system requires substantially fewer disclosures and assumes that judges are best positioned to direct the process.[29] The comparatively narrower scope of the disclosures required in Chinese courts and the comparatively more active role of the judiciary further illustrates the inverse legal privacy paradigms in the U.S. and China.

The U.S. and China have inversely disjunctive views concerning data privacy from government and data privacy from commercial entities.[30] The two countries' constitutions illustrate their discordant concepts surrounding the question of from whom one shall remain private. The Fourth Amendment to the U.S. Constitution protects individuals from governmental intrusions.[31] The U.S. Supreme Court's

---

[25] *Sedona Discovery & Data Protection*, *supra* note 21, at 405.

[26] *Id.* at 406.

[27] *Id.*

[28] Plata v. Brown, 754 F.3d 1070, 1078 (9th Cir. 2014).

[29] *Infra* at 9–10 (explaining the evidence exchange process in Chinese courts).

[30] *See generally* Samm Sacks & Lorand Laskai, *China's Privacy Conundrum*, SLATE: FUTURE TENSE (Feb. 7, 2019), https://slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html. The authors describe as a "conundrum" the privacy laws in China that protect individuals' data from private entities while allowing the government increasingly unfettered access to the same data. They also explain that the U.S. has an inverse "conundrum" because the Supreme Court provides "fairly strong privacy protections against government data collection," while "the country still lacks a comprehensive consumer privacy law." *Id.*

[31] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

interpretation of that Amendment provides comparatively[32] strong protection for individuals from government data collection.[33] Though guaranteeing broad protections from governmental intrusions into individuals' privacy, the U.S. lags behind other nations in passing laws that protect individuals' data from non-governmental entities.[34]

Although China's protections surpass the commercial data protections afforded by U.S. laws,[35] the Chinese government's access to individuals' data would run afoul of the U.S. Constitution.[36] The Chinese constitution explicitly provides individuals a right to privacy from private individuals and organizations: "Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe on citizens' freedom of privacy of correspondence."[37] However, the protection does not extend to protection from government intrusions. Article 40 provides a right to privacy "except in cases where, to meet the needs of State security or of criminal investigation, public security or prosecutorial organs are permitted to censor correspondence in accordance with the procedures prescribed by law."[38] Thus, individuals in China have a constitutional right to maintain their privacy, free from the intrusion of individuals or commercial

[32] *See infra* at 8 (discussing the Chinese government's basically unfettered ability to collect its citizens' data).

[33] *See* Carpenter v. United States, 138 S. Ct. 2206 (2018) (holding that individuals maintain an expectation of privacy in cell-site location information and holding that the state generally must first obtain a warrant before gathering the information from third parties).

[34] California recently passed legislation granting consumers more control over their data privacy than federal laws afford, but even that law is not as expansive as the GDPR and similar guidelines. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018); CAL. CIV. CODE § 1798.100 (West 2020).

[35] *See* Sacks & Laskai, *supra* note 30.

[36] One example of the government's eerie use of data is the "social credit" scheme. Christina Zhao, *'Black Mirror' In China? 1.4 Billion Citizens to be Monitored Through Social Credit System*, NEWSWEEK (May 1, 2018), https://www.newsweek.com/china-social-credit-system-906865. The program, which the government hopes to fully unleash in 2020, gives social credit scores to individuals based on certain character traits, like volunteerism and loyalty to China. *Id.* The government uses individuals' data to calculate the scores. *Id.* Low scores potentially result in restrictions on travel. *Id.*; *see also Planning Outline for the Construction of a Social Credit System (2014–2020)*, CHINA COPYRIGHT AND MEDIA (last updated Apr. 25, 2019), https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/.

[37] XIANFA art. 40 (2007) (China), http://www.npc.gov.cn/zgrdw/englishnpc/Constitution/2007-11/15/content_1372964.htm.

[38] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

entities, but the right does not extend to the right to maintain privacy from governmental intrusions.

Samm Sacks, a cybersecurity fellow at New America, suggests that the rate of increased government surveillance in China trends towards total governmental surveillance.[39] The Chinese government already has a "vast, secret system of advanced facial recognition technology," and uses the system to monitor protestors in Hong Kong[40] and track ethnic populations in mainland China.[41] As China leads the world in curtailing commercial surveillance of individuals' data,[42] the Chinese government maintains virtually unfettered access to personal data.[43]

Underlying the U.S. pretrial discovery process and China's evidence disclosure process are starkly different legal privacy paradigms. The U.S. entrusts litigants to manage the process with the goal of having "mutual knowledge of all the relevant facts" before the trial begins.[44] In China, practitioners rely almost exclusively on the judiciary to determine what evidence is needed, what evidence parties must produce, and to what evidence litigants may be privy.[45] The above practices are thus illustrative of the two legal systems' divergent concepts of privacy and the role of government.

3. Evidence Collection Process in China

The U.S. offers the broadest form of pretrial evidence exchange across national jurisdictions, and it differs greatly from the process in China.[46] While Chinese laws

---

[39] Sacks & Laskai, *supra* note 30.

[40] Zach Doffman, *Hong Kong Exposes Both Sides of China's Relentless Facial Recognition Machine*, FORBES (Aug. 26, 2019), https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/#50d3c96e42b7.

[41] *Id.*; Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (April 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

[42] "These actions on privacy issues have turned China into 'a surprise leader in Asia on data privacy rules.'" Sacks & Laskai, *supra* note 30.

[43] *See* Zhizheng Wang, BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA IN CHINA 248 (2017) (describing the Basic Internet Database, a database in which the Chinese government stores data it collects from internet service providers concerning users' accounts and other data of interest to the government).

[44] Hickman v. Taylor, 329 U.S. 495, 507 (1947).

[45] *China and the United States*, *supra* note 18, at 283–94.

[46] *See id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

do not authorize a U.S.-style discovery procedure, Chinese laws regulate a system of evidence disclosure in which "judges must carefully examine case materials and investigate and collect necessary evidence."[47] Judge Tao, a judge on the High People's Court of Beijing Municipality, explains that the phrase "investigating and collecting evidence" best describes the process.[48]

Before litigation begins, litigation representatives[49] may "investigate and collect evidence."[50] Before filing a complaint, litigants should obtain relevant evidence to attach to their complaints.[51] No particular law clearly regulates how parties collect evidence.[52] The law provides general principles, but lacks details concerning proper procedures and how litigation representatives can protect their general rights to collect evidence.[53] Though litigation representatives have the right to collect evidence and interview witnesses, there is no enforcement mechanism in Chinese courts that can compel the witnesses to produce the information the litigation representatives request.[54] Additionally, in the Chinese process, parties lack the power to collect evidence from third parties.[55]

Due to parties' limited power and expertise, Chinese judges are at the forefront of the evidence gathering process. Judges actively investigate matters and collect evidence they deem necessary to fairly resolve the dispute.[56] Because litigants have little legal awareness and limited mechanisms to compel adversaries to disclose

---

[47] Zhonghua Renmin Gongheguo Minshi susong fa [Civil Procedure Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 31, 2012, effective Aug. 31, 2012) 2012, art. 129.

[48] *Id.* at 2.

[49] Though lawyers represent litigants most frequently in China, other types of professionals also serve as "litigation agents." *China and the United States*, *supra* note 18, at 283.

[50] *Id.* at 283 n.14.

[51] *Id.* at 285. The evidence requirement at the complaint stage is a bit unclear. Judge Tao explains that most litigants are ill informed of the legal system and rely on judges to explain the procedures and investigate the claims. *Id.* at 286. She explains that if judges believe that litigants have produced insufficient evidence in support of their theory of the case, the judge will ask the party to offer more relevant evidence. *Id.*

[52] *Id.* at 284.

[53] *Id.* at 296.

[54] *Id.* at 285.

[55] *Id.* at 297.

[56] *Id.* at 288–94.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

evidence, the role of the judge overshadows the role of the parties.[57] Arguably, the judges fulfill the role of fact collector rather than fact finder.[58]

The limited role of the litigants during the Chinese pretrial "investigating and collecting of evidence" process contrasts sharply with discovery in U.S. federal courts, where the litigants conduct discovery under the supervision of the courts.[59] Moreover, unlike the sparse Chinese laws governing the "investigation and collection of evidence" process, the FRCP strictly regulate the pretrial discovery process in U.S. courts.[60] And while litigants lack any ability to compel adversaries to comply with their investigations under Chinese law, the FRCP provide parties with many tools they can utilize to enforce their rights to evidence under U.S. law.[61]

Just as the inverse legal privacy paradigms generally underlie the differences in the evidence exchange processes in China and the U.S., the differences in the discovery processes underlie the clash that occurs when the two jurisdictions meet in the realm of pretrial discovery. When discoverable data under U.S. laws is stored in China, conflicts arise. The U.S. courts' presumption that broad discovery begets just outcomes collides with the limited power litigants have to collect evidence in China and the relatively stronger protections Chinese laws provide to those who seek to maintain privacy from non-governmental actors.

4. The Hague Evidence Convention

Disputes arise when the vast U.S. discovery process attempts to sweep up ESI stored in countries with fundamentally different concepts of privacy and pretrial evidence exchange.

Fifty-nine countries—including the U.S., and China, with reservations—signed the Hague Evidence Convention ("Hague Convention").[62] Lawyers in the U.S.

---

[57] *Id.* at 294.

[58] *Id.*

[59] SEDONA CONFERENCE, INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA FOR ADDRESSING THE U.S. LITIGATION: TRANSITIONAL ADDITION (Denise E. Backhouse ed., 2017), https://thesedonaconference.org/sites/default/files/publications/International%2520Litigation%2520Principles_Transitional%2520Ed_Jan%25202017.pdf [hereinafter SEDONA PRINCIPLES ON DISCOVERY].

[60] *See* FED. R. CIV. P. 26.

[61] *See* FED. R. CIV. P. 36.

[62] Hague Conference on Private International Law, Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555 [hereinafter Hague Convention]; Hague Conference on Private Int'l Law, *Status Table: 20: Convention of 18 March 1970 on the Taking of*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

encouraged American involvement in the Hague Convention to "improve the process of obtaining evidence abroad."[63] At the time, U.S. litigants increasingly sought evidence stored abroad.[64] They encountered problems when they sought evidence from countries with very different legal systems.[65] When litigants attempted to gather the evidence stored abroad, they encountered governments with varying dispositions to cooperate and substantially different processes for obtaining the evidence.[66] The U.S. signed the Hague Convention to remedy these problems that arose in "the absence of a treaty or convention regulating the matter."[67] The signatories desired to "improve mutual judicial co-operation in civil or commercial matters."[68] The Hague Convention provided a way to mitigate discovery issues that tended to arise frequently when cases involved litigants from both civil and common law countries.[69] The Hague Convention established "methods of co-operation for the taking of evidence abroad in civil or commercial matters,"[70] creating an alternative system that accommodates the differences in the civil and common law evidence exchange systems.[71]

Under the Hague Convention, when parties seek evidence stored in a foreign jurisdiction during pretrial discovery, the presiding court issues a letter of request to the designated central authority in the nation where the data is stored.[72] When a litigant in a U.S. court seeks to obtain evidence stored in China through the Hague

---

Evidence Abroad in Civil or Commercial Matters, HCCH, https://www.hcch.net/en/instruments/conventions/status-table/?cid=82 [https://perma.cc/7QND-B72S].

[63] Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 530 (1987).

[64] *Id.* at 531 (citations omitted).

[65] *Id.*

[66] *Id.* "Some countries have insisted on the exclusive use of the complicated, dilatory and expensive system of letters rogatory or letters of request. Other countries have refused adequate judicial assistance because of the absence of a treaty or convention regulating the matter." *Id.*

[67] *Id.*

[68] Hague Convention, *supra* note 62.

[69] *Id.*; *see also* Maggie Gardner, *Parochial Procedure*, 69 STAN. L. REV. 941, 968 (2017).

[70] HCCH, CONVENTION OF 18 MARCH 1970 ON THE TAKING OF EVIDENCE ABROAD IN CIVIL OR COMMERCIAL MATTERS: OUTLINE EVIDENCE CONVENTION (last visited Nov. 15, 2020), https://assets.hcch.net/docs/ec1fc148-c2b1-49dc-ba2f-65f45cb2b2d3.pdf.

[71] *Id.*

[72] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

Convention, the presiding judge in the U.S. court submits a letter to the Ministry of Justice of the People's Republic of China ("MOJ"), the Chinese Central Authority.[73] The MOJ forwards the letter to the court in the district in which the evidence is stored.[74] The lower court then serves the letter on the party from whom the U.S.-based litigant is requesting production of the evidence.[75] The evidence is produced to the presiding judge in the U.S. court through the same channel.[76] Letters of request can take up to a year to be fully executed.[77] The practical aspects of the process in China are largely unknown, including how long most requests take on average, because China has been reluctant to share information about its process.[78]

Utilization of the Hague Convention procedures may create an avenue for requesting parties to receive their desired data without forcing the party with control of the data to violate foreign privacy laws. Because the designated central authority in each jurisdiction processes the letter of request, the party or nonparty with control of the data is not individually responsible for its production.[79] However, as previously stated, the letter of request, which should be executed "expeditiously," may take up to a year to process,[80] potentially delaying litigation beyond what may be practical. The process may not lead to positive results for the party seeking production of data stored within China's borders.[81]

B. U.S. Courts' Weighing of Discovery Laws and Foreign Privacy Laws

Cross-border discovery conflicts arise when U.S. courts determine that a party or nonparty has sufficient "control" over ESI to warrant production in the U.S.[82] and

[73] Minning Yu, *Benefit of the Doubt: Obstacles to Discovery in Claims Against Chinese Counterfeiters*, 81 FORDHAM L. REV. 2987, 3000 (2013).

[74] *Id.*

[75] *Id.*

[76] *Id.* at 3001.

[77] *Id.*

[78] *Id.*

[79] Hague Convention, *supra* note 62. *See* Proskauer Rose LLP, *International Litigation: Requesting Discovery Abroad for US Proceedings*, PRACTICAL LAW (2019).

[80] Yu, *supra* note 73, at 3001.

[81] Wultz v. Bank of China Ltd., 910 F. Supp. 2d 548, 558 (S.D.N.Y. 2012).

[82] "A party may serve on any other party a request within the scope of Rule 26(b): (1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

the data is simultaneously subject to foreign data protection laws.[83] Although U.S. courts have the authority to order production of the ESI sought, even if foreign laws preclude legal transfer,[84] the judicial principle of international comity inhibits the unrestricted exercise of this power, and instructs courts to consider the foreign data privacy law.[85] However, comity is only one factor that U.S. courts balance in deciding whether to exercise their power to compel discovery.

The principle of judicial comity informs U.S. courts' decisions when they encounter foreign laws. U.S. jurisprudence has recognized comity since the 1800s.[86] In 1895, the Supreme Court of the United States explained that the elusive concept,

> in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons who are under the protection of its laws.[87]

The United States Court of Appeals for the District of Columbia Circuit explained that because courts' consideration of comity varies depending on the factual circumstances surrounding each claim, the duties the principle imposes in a given dispute are uncertain.[88] But the inherent edict of comity instructs U.S. courts to give foreign laws effect when appropriate to foster international cooperation and reciprocity.[89]

In *Aérospatiale*, the U.S. Supreme Court specifically considered what a federal trial court should do if a party sought discovery of material located abroad, in a

---

responding party's possession, custody, or control: . . . electronically stored information." FED. R. CIV. P. 34.

[83] SEDONA PRINCIPLES ON DISCOVERY, *supra* note 59, at 5.

[84] Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 546 (1987).

[85] *Id.*

[86] Hilton v. Guyot, 159 U.S. 113, 163–64 (1895).

[87] *Id.*

[88] Laker Airways Ltd. v. Sabena, Belgian World Airlines, 731 F.2d 909, 937 (D.C. Cir. 1984).

[89] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

country whose law blocked discovery of the material.[90] Under *Aérospatiale*, federal courts must balance five 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.[91]

In *Aérospatiale*, victims of an airplane crash in Iowa brought personal injury claims against airplane manufacturers owned by the French government.[92] The defendants alleged that the magistrate judge in the United States District Court for the Southern District of Iowa should have pursued the Hague Evidence Convention rather than the FRCP in seeking discovery of material located in France.[93] After initially cooperating in discovery, the French defendants filed a motion for a protective order alleging that the Hague Convention exclusively governed the procedure for pretrial exchange of evidence located in France.[94] The Supreme Court held that the text of the Hague Convention did not demand exclusive reliance on its procedures, and interpreting it as such "would subordinate the court's supervision of even the most routine of these pretrial proceedings to the actions or, equally, to the inactions of foreign judicial authorities."[95]

The Court held that rather than rely exclusively on the Hague Convention procedures, U.S. courts should engage in a particularized analysis of the interests of the foreign nation and the U.S.[96] The Court explained that the Restatement of Foreign Relations Law of the United States delineated the relevant comity test in determining

---

[90] Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522 (1987).

[91] *Id.* at 544 n.28 (quoting RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 (AM. LAW INST. 1987)).

[92] *Aérospatiale*, 482 U.S. at 521.

[93] *Id.* at 526.

[94] *Id.*

[95] *Id.* at 539.

[96] *Id.* at 544.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

when U.S. courts should exercise their power to order foreign discovery in the face of foreign objections.[97] In addition to the five-factor balancing test, the Court instructed U.S. courts to "exercise special vigilance" during pretrial proceedings in order to shield foreign parties from onerous discovery[98] and 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."[99] While U.S. courts must consider problems foreign litigants may encounter and respect the expressed interest of foreign states, the Supreme Court did "not articulate specific rules to guide this delicate task of adjudication."[100] Some lower courts have criticized the lack of specific instructions in *Aérospatiale*.[101] The lack of specificity in the Court's ruling could account for the tendency of U.S. courts to resolve disputes in favor of discovery under the FRCP rather than more heavily weighing the interests of foreign jurisdictions.[102]

Justice Blackmun foreshadowed the conflict, warning in his partial dissent in *Aérospatiale* that domestic judges were ill-equipped to balance American and foreign interests and would likely default to domestic procedures.[103] After *Aérospatiale*, some of the United States Courts of Appeals added an additional prong to the balancing test that requires parties responding to discovery requests who would prefer to proceed under the Hague Convention rather than comply directly under the FRCP to show that they would likely experience harm if they complied with the production request,[104] making it more difficult for those parties to prove that the Hague Convention is the proper discovery method. Additionally, some courts may

[97] *Id.* 544 n.28.

[98] *Id.* at 546.

[99] *Id.*

[100] *Id.*

[101] "Regrettably, the Court [in *Aérospatiale*] declined to set forth specific rules to guide such exercise of judicial discretion." Scarminach v. Goldwell GmbH, 531 N.Y.S. 2d 188, 189 (Sup. Ct. Monroe Co. 1988).

[102] One commentator explains that the lack of specific instructions from the Supreme Court empowered lower courts to discount foreign interests without the proper degree of scrutiny. Diego Zambrano, *A Comity of Errors: The Rise, Fall, and Return of International Comity in Transnational Discovery*, 34 BERKELEY J. INT'L L. 157, 175 (2016).

[103] *See* Gardner, *supra* note 69, at 970.

[104] *See* David Moncure, *The Conflict Between United States Discovery Rules and the Laws of China: The Risks Have Become Realities*, 16 SEDONA CONF. J. 283, 299–300 (2015).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

weigh whether litigants acted in bad faith during the discovery process as part of their analysis.[105]

Following *Aérospatiale*, courts have overwhelmingly relied on the FRCP rather than the Hague Convention—tipping the scale to the side of vast U.S. discovery.[106] When discovery disputes have arisen involving ESI stored in China, U.S. courts have largely followed this trend of ordering production under the FRCP.[107]

C. E-Discovery Disputes Involving ESI Stored in China Before China's Personal Data Privacy Overhaul

Before the recent overhaul, Chinese data protection provisions were peppered throughout various statutes and regulations and created challenges when litigants in U.S. courts sought ESI stored in China.[108] Even before enactment of the new regulations, U.S. courts recognized the difficulty of discovering materials stored in China.[109] When U.S. courts issued discovery orders involving ESI stored in China, they employed the *Aérospatiale* analysis. A court's decision to follow the Hague Convention procedure rather than the FRCP had major consequences for litigants regarding discoverable ESI. In 1998, China adopted a reservation under the Hague Convention stipulating that it would only execute pre-trial discovery requests that "are of direct and close connection to the subject matter of the litigation."[110] The "direct and close connection" standard China announced is more circumscribed than the Rule 26(b)(1) standard, which declares as potentially discoverable any "nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case."[111] If the court opts to use the Hague Convention, the scope of discovery will be much more narrow than under the FRCP.

---

[105] Tiffany (NJ) LLC v. Andrew, 276 F.R.D. 143, 160 (S.D.N.Y. 2011).

[106] *See* Zambrano, *supra* note 102, at 177–78.

[107] *See infra* Section I.C.

[108] Daley et al., *supra* note 5, at 240.

[109] In an opinion granting final approval of a settlement agreement, the U.S. District Court for the District of New Jersey based its approval in part on the difficulty plaintiffs would face in acquiring evidence located in *China. P. Van Hove BVBA v. Universal Travel Grp., Inc.*, No. CV 11-2164, 2017 WL 2734714, at *8 (D.N.J. June 26, 2017). *See also* Dartell v. Tibet Pharm., Inc., No. CV 14-3620, 2017 WL 2815073 (D.N.J. June 29, 2017).

[110] *Tiffany*, 276 F.R.D. at 160.

[111] FED. R. CIV. P. 26(b)(1).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

But even if the court declines to use the Hague Convention procedures, it may nevertheless deny discovery of ESI otherwise discoverable under the FRCP.[112]

Preceding the promulgation of the Cybersecurity Law and the Specification, the United States District Court for the Southern District of New York issued a series of opinions related to the discovery of information from the Bank of China (BOC).[113] In each case, a party litigating in the Southern District of New York sought evidence stored in China in the possession of the Bank of China.[114] In each case, the BOC sought discovery under the Hague Convention rather than the FRCP due to restrictive Chinese bank secrecy laws that forbade the bank from producing the documents to the litigants in U.S. courts.[115] In each case, the court applied the Second Circuit's seven-factor comity test, which includes the five-factor *Aérospatiale* test as well as two additional factors: 1) potential harm the producing party would suffer if it complied with the discovery request, and 2) whether the party has proceeded in good faith.[116]

1. *Tiffany v. Andrew* (S.D.N.Y. 2011)

In a trademark infringement action filed in the Southern District of New York, the court weighed the comity factors and ultimately concluded that the Hague Convention procedures were the appropriate means for discovering documents of which BOC, a nonparty in the case, had possession.[117] The court found that BOC had presented sufficient evidence to establish that Hague Convention procedures in China had recently improved and the Chinese Ministry of Justice had recently been more willing to execute a request for documents under the Convention.[118] The court

[112] The U.S. District Court for the Southern District of New York denied a motion to compel discovery of ESI created by the Chinese government. Wultz v. Bank of China Ltd., 942 F. Supp. 2d 452, 473 (S.D.N.Y. 2013).

[113] Moncure, *supra* note 104, at 299–300.

[114] *Id.*

[115] *Id.* The bank secrecy laws invoked by the Bank of China in the cases in the Southern District of New York refer to a "multitude of civil and criminal regulations" China enacted to protect "bank customers' privacy and encouraging use of, and confidence in, [China's] relatively new banking system." *Tiffany*, 276 F.R.D. at 160.

[116] Moncure, *supra* note 104, at 300.

[117] *Tiffany*, 276 F.R.D. at 160–61.

[118] *Id.* at 160.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

found that the Chinese interest in protecting bank secrecy laws outweighed the U.S. interest in enforcing intellectual property rights.[119]

The next month in *Gucci America, Inc. v. Weixing Li*, a different judge in the Southern District of New York disagreed with the court's finding in *Tiffany* that the Chinese Ministry of Justice had exhibited an increased willingness to execute requests for documents under the Hague Convention.[120] The court in *Gucci* explained that although there were similar factual circumstances in *Tiffany* and *Gucci*, and BOC put forward similar evidence in both cases, the *Gucci* court found that a request pursuant to the Hague Convention would be futile.[121] The *Tiffany* and *Gucci* opinions represent the uncertainty and variance of how courts ultimately decide whether or not to exert their power to compel production of ESI stored in China under the FRCP.

2. *Gucci v. Li* (S.D.N.Y. 2011)

In *Gucci v. Weixing Li*, clothing designer Gucci brought a trademark infringement action against a Chinese website, which sold allegedly infringing items.[122] The Chinese website had bank accounts with BOC, a nonparty to the suit.[123] The plaintiffs sought ESI from BOC they deemed "critical to their investigation of the Defendants' alleged counterfeiting operations."[124] BOC refused to produce any documents stored in China, claiming that Chinese bank secrecy laws forbade production.[125] In response, Gucci filed a motion to compel BOC to produce the documents.[126] The United States District Court for the Southern District of New York, relying on the FRCP, granted the motion.[127]

The court weighed the *Aérospatiale* factors and ultimately rejected BOC's argument that any discovery of documents stored in China should be pursued via the

---

[119] *Id.*

[120] Gucci Am., Inc., v. Weixing Li, No. 10 CIV. 4974(RJS), 2011 WL 6156936, at *9 (S.D.N.Y. Aug. 23, 2011), *vacated*, 768 F.3d 122 (2d Cir. 2014).

[121] *Id.*

[122] *Id.* at *1.

[123] *Id.*

[124] *Id.*

[125] *Id.* at *5.

[126] *Id.* at *2.

[127] *Id.* at *5, *13.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

Hague Convention.[128] BOC argued that because producing the ESI stored in China "could subject the [b]ank to civil and criminal liability, the appropriate way for Plaintiffs to make a request for documents is through the Hague Convention."[129] BOC argued that the Hague Convention procedures served as an adequate alternative to discovery under the FRCP.[130] BOC presented evidence that the State Department had recently removed a statement on its website saying Hague Convention procedures to obtain documents stored in China "had not been particularly successful in the past."[131] BOC also explained that in the *Tiffany* opinion, the court had weighed the "alternative means" factor in favor of the Hague Convention procedures in light of the removal of the State Department statement.[132]

The *Gucci* court rejected BOC's argument, explaining that the plaintiff had presented sufficient evidence that the Hague Convention in China had been unsuccessful in the past, and BOC had not presented sufficient evidence to refute its argument.[133] Moreover, the court found the plaintiff presented sufficient evidence to support a conclusion that there was unlikely an alternative method of securing the documents requested if the court did not utilize its power under the FRCP.[134] The court explained that "the mere fact that the Hague Convention provides an alternative method for obtaining the documents is not proof that it is necessarily an effective, or efficient, method for doing so in this case."[135] Ultimately, the court concluded that the Hague Convention procedures would be unlikely to effectuate production of the documents.

The court also weighed each country's national interests. It found that the U.S.'s interest in enforcing its intellectual property laws, which were essential to the counterfeiting case, and in the U.S. policies favoring broad discovery outweighed China's interest in enforcing its bank secrecy laws.[136] The court explained that

---

[128] *Id.* at *5–13.

[129] *Id.* at *5.

[130] *Id.*

[131] *Id.* at *9.

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *Id.* at *8 (quoting *In re* Air Cargo Shipping Servs. Antitrust Litig., 278 F.R.D. 51, 52 (E.D.N.Y. 2010)).

[136] *Id.* at *11.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

China's interests were outweighed because there were many exceptions to Chinese bank secrecy laws in practice.[137] China's national interest was further undercut by the suggestion that "China's bank secrecy laws merely confer an individual privilege on customers rather than reflect a national policy entitled to substantial deference."[138] Additionally, the court noted that the defendants in the action had allegedly strategically used BOC to facilitate global infringement schemes, highlighting the fact that the secrecy laws were being utilized to evade U.S. laws and discrediting the notion of legitimate Chinese interest in enforcing its bank secrecy laws.[139]

In balancing the hardship of compliance, the *Gucci* court weighed the *Aéropostiale* factors in favor of the plaintiffs who sought production of the evidence stored in China under the FRCP. The court found BOC's "representation of the liability that it faces to be unduly speculative."[140] BOC contended that it could be subjected to civil and criminal liabilities if it was forced to produce the bank records under the FRCP.[141] It pointed to Chinese case law demonstrating the civil liabilities the bank had been subjected to in domestic matters.[142] However, the court rejected BOC's argument as overly speculative because BOC could not point to a single instance "in which a Chinese financial institution was punished for complying with a foreign court order directing the production of documents."[143] Thus, because the defendants did not present sufficient evidence supporting their expectant hardship of compliance, the factor weighed in favor of the plaintiffs.

The *Gucci* opinion represents the power of the U.S. federal courts to compel a nonparty in an action to produce ESI stored in China even when Chinese laws deem the production illegal. The court's analysis of China's laws shows that courts are willing to look beyond the text of a foreign law and analyze how the law works in the foreign country. Finally, the court seemed to denigrate Chinese laws because they aim to provide a privacy privilege to customers rather than to protect broad national interests.

---

[137] *Id.* at *10.

[138] *Id.*

[139] *Id.*

[140] *Id.* at *11.

[141] *Id.*

[142] *Id.*

[143] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

3. *Wultz v. Bank of China* (S.D.N.Y. 2011–2013)

After *Gucci*, the Southern District of New York flipped between analyzing discovery requests under the Hague Convention and the FRCP in a series of decisions made in the *Wultz v. Bank of China* case.[144] Originally in 2011, the Southern District of New York granted BOC's request to respond to discovery requests under the Hague Convention,[145] only to reverse itself in 2012 ordering BOC to produce the same bank records under the FRCP.[146] The court's course reversal illustrates the impact of the *Gucci* court's appraisal that the Hague Convention may not be a viable alternative to production under the FRCP when a party seeks ESI stored in China.

In *Wultz v. Bank of China*, family members of victims of a 2006 suicide bombing brought a claim against BOC for allegedly financing the terrorist organization responsible for the attack.[147] In 2011, Southern District of New York granted the defendant, BOC's, request to follow the Hague Convention.[148] On August 31, 2011, the court issued a Letter of Request to the Chinese Ministry of Justice.[149] However, the MOJ did not timely respond to the court's Letter of Request under the Convention and did not produce the documents.[150]

In response to the Ministry's failure to comply with the Letter of Request, the plaintiffs filed a motion in 2012 to compel production of the bank records under the FRCP.[151] In support of their motion, the plaintiffs presented evidence indicating that even if the MOJ did eventually fulfill the request, it would likely refuse to produce documents crucial to the litigation.[152] The 2012 opinion and unfolding of the discovery process shows that courts at times prefer the bilateral Hague Convention

[144] Wultz v. Bank of China Ltd., 910 F. Supp. 2d 548 (S.D.N.Y. 2012); Wultz v. Bank of China Ltd., 942 F. Supp. 2d 452 (S.D.N.Y. 2013).

[145] *Wultz*, 910 F. Supp. 2d at 551.

[146] *Id.* at 561.

[147] *Id.* at 551.

[148] *Id.*

[149] *Id.*

[150] *See id.* at 558 ("The time that has already passed since this Court's submission of the Letter of Request on August 31, 2011, by itself calls into question whether the Hague Convention process can be viewed as a reasonable alternative means of discovery.").

[151] *Id.* at 550.

[152] *Id.* at 558.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

procedure to the procedures under the FRCP. While the court opined that "bilateral mechanisms are preferable to unilateral actions in cross-border legal enforcement,"[153] it nevertheless explained that it must act unilaterally under the factual circumstances and exercise its power to compel production of ESI stored in a foreign jurisdiction blocked by foreign laws.[154] It concluded that, due to the inaction of the MOJ and the probable refusal of the Ministry to produce the requested evidence, the Hague Convention was not "a viable alternative method of securing the information Plaintiffs" sought.[155] As a result, the court granted the plaintiffs' motion to compel under the FRCP.[156]

Instead of complying with the 2012 order, BOC refused to provide the requested documents, reiterating that it was precluded from doing so under Chinese bank secrecy and anti-money laundering laws.[157] In response, the Southern District of New York again considered plaintiffs' motion to compel BOC to produce ESI stored in China in 2013.[158] BOC argued once more that Chinese banking laws prohibited it from producing the documents.[159] Applying the FRCP, the court ordered BOC to produce all documents discoverable under the FRCP, except relevant documents under BOC's control created by the Chinese government.[160] The court limited the discovery requests by requiring BOC to produce the documents to the court solely for an in camera review.[161] By limiting the discoverable materials between BOC and the Chinese Government and requiring in camera review, the discovery order shows that even when courts apply the FRCP, they will consider the foreign sovereign's interest—as directed by the United States Supreme Court in *Aérospatiale*.

The court's analysis shows it may not weigh individual privacy interests as heavily as other state interests. The United States District Court for the Southern District of New York explained that in balancing the protections due to BOC, the

[153] *Id.* at 557.

[154] *Id.*

[155] *Id.*

[156] *Id.* at 560.

[157] Wultz v. Bank of China Ltd., 942 F. Supp. 2d 452, 457 (S.D.N.Y. 2013).

[158] *Id.* at 455.

[159] *Id.*

[160] *Id.* at 473.

[161] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

party potentially responsible for producing ESI stored in China, laws "primarily concerned not with protecting the confidentiality of bank clients, but with combating money laundering and other illegal financial transactions" would offer stronger protection to BOC.[162]

These motions to compel demonstrate that preceding China's passage of the Cybersecurity Law and Specification, a foundational conflict between U.S. and Chinese law already existed when litigants in U.S. courts sought production of evidence stored in China. First, individuals in the two countries have vastly different privacy rights. Individuals in China have more protection from commercial entities while individuals in the United States have greater protection from governmental intrusions. Second, the two countries have vastly different systems of evidence disclosures. In the U.S., individual litigants participate in the world's broadest pre-trial discovery system, while in China, judges control the relatively limited process of "investigation and collection of evidence."[163] These differences underlie the conflict illustrated in the series of opinions from the Southern District of New York. In each of the cases, plaintiffs in U.S. courts sought evidence stored in China. And the entity with possession of the evidence argued that it could not produce the documents because production would be illegal under Chinese privacy laws.

In the absence of reforms, these opinions illustrate that production under the Hague Convention is unlikely to be a reliable method of receiving data stored in China. Moreover, the opinions illustrate the trend in U.S. courts to order production of evidence stored in China, even when Chinese privacy laws forbid production and production would subject litigants to liabilities. The *Gucci* opinion shows that courts are unlikely to weigh evidence of potential harm in favor of production under the Hague Convention, unless litigants point to harms experienced by similarly situated litigants in cross-border evidence disclosures. The court will also likely favor production under the FRCP when the Chinese laws in question purport to protect personal privacy interests rather than broad state interests. Consequently, these fundamental differences between China and the U.S. before the promulgation of the Cybersecurity Law and Specification, and how courts have traditionally balanced the comity factors, suggest that China's passage of major personal privacy laws and regulations will likely not alter how U.S. courts analyze discovery disputes involving ESI stored in China when production is blocked by Chinese privacy laws.

---

[162] *Id.* at 467, 458–59.

[163] *See China and the United States*, *supra* note 18.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

II. CHINA'S NEW DATA PRIVACY SYSTEM AND ITS EFFECT ON E-DISCOVERY DISPUTES

A. Overhaul of China's Data Privacy Laws and Regulations

The National People's Congress of China adopted the Cybersecurity Law of the People's Republic of China ("The Cybersecurity Law") in 2016,[164] marking the beginning of the data privacy renaissance in China. The Cybersecurity Law summarizes the basic principles of personal information protection, and the Specification, passed two years later, provides more specific guidelines for stakeholders.[165]

The Cybersecurity Law requires that all citizens' personal information data be stored in mainland China.[166] Both the Cybersecurity Law and Specification broadly define sensitive personal information as any data that has the potential to cause harm if it were to be lost or misused, rather than based on a specific type of data.[167] The data localization laws have affected how entities conduct business within China and with Chinese based businesses and organizations.[168] For example, the New York Times published an article following the promulgation of the Cybersecurity Law, detailing Apple's plans to build a data center in China.[169] It explained that other international tech companies, including Airbnb, were in the process of building data centers in China to comply with the Cybersecurity Law.[170] The necessity of building data centers in China illustrates the added burden the data localization laws have placed on conducting business in China.

---

[164] *Cybersecurity Law*, *supra* note 7.

[165] *Id.*; *see* Wei Sheng, *One Year After GDPR, China Strengthens Personal Data Regulations, Welcoming Dedicated Law*, TECHNODE (June 19, 2019), https://technode.com/2019/06/19/china-data-protections-law/.

[166] *Cybersecurity Law*, *supra* note 7, at art. 37; *see also* Elizabeth Cole et al., *Implementing China's Cybersecurity Law*, JONES DAY WHITE PAPER, Aug. 2017, at 1, 4, https://www.jonesday.com/files/upload/Implementing%20Chinas%20Cybersecurity%20Law.pdf.

[167] Yan Luo & Phil Bradley-Schmieg, *China Issues New Personal Information Security Standard*, COVINGTON: INSIDE PRIVACY (Jan. 25, 2018), https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard/.

[168] *See* Paul Mozur, Daisuke Wakabayashi & Nick Wingfield, *Apple Opening Data Center in China to Comply with Cybersecurity Law*, N.Y. TIMES (July 12, 2017), https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html.

[169] *Id.*

[170] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

Furthermore, the Court of Appeals for the District of Columbia issued a memorandum opinion ordering Google to comply with a warrant requiring Google to disclose to the U.S. government records and information stored abroad associated with a particular Google account.[171] In the opinion, the judge warned of the potential negative effect of data localization laws on criminal investigations,[172] explaining that by restricting where data may be stored, the Chinese government may protect its citizens from the reach of U.S. law enforcement.[173] Consequently, these examples may also serve as a caution for civil litigants. As businesses store increasingly more data in China to comply with the new data security laws, there is a greater chance that data relevant to future litigation will be stored in China than there was preceding the data localization laws, potentially increasing the prevalence of cross-border discovery disputes involving data stored in China.

The Cybersecurity Law contains broad requirements, and it has thus received criticism for its lack of specifics[174] and perceived protectionism.[175] In response, China's National Information Security Standardization Technical Committee ("TC260") issued the Personal Information Security Specification in March of 2018.[176] The Specification provides detailed guidance for collecting, storing, using,

---

[171] *In re* Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-MJ-00757 (BAH), 2017 WL 3445634, at *1 (D.D.C. July 31, 2017).

[172] *Id.* at *27.

[173] *Id.*

[174] *See* Michael Kan, *China's Vague Cybersecurity Law Has Foreign Businesses Guessing*, COS (Nov. 8, 2016), https://www.csoonline.com/article/3137248/chinas-vague-cybersecurity-law-has-foreign-businesses-guessing.html ("The most disturbing thing for foreign businesses facing China's new cybersecurity law may just be how vague and broad it is."); Drew Foerster, *China's Legislature Gears Up to Pass A Sweepingly Vague Cybersecurity Law*, ABA: BUS. L. TODAY (May 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/05/02_foerster/.

[175] *See* Kan, *supra* note 174 (While the law superficially promotes cybersecurity, industry leaders doing business in China have complained that it is another step in line with China's protectionist tendencies—Chinese policies that favor Chinese businesses over foreign business. Another critique explained that the data localization requirements, combined with the vagueness of the law, could lead to increased access to foreign businesses' data by the Chinese government.); *see also* Daniel Wagner, *China's Cybersecurity Law Is Biased and Open To Abuse, But It May Not Stop Others Copying It*, SOUTH CHINA MORNING POST (June 25, 2018), https://www.scmp.com/comment/insight-opinion/china/article/2152347/chinas-cybersecurity-law-biased-and-open-abuse-it-may ("The vagueness of this provision, as well as undefined concepts of national security and public interest contained within the law, increases the government's grounds to assert the need for investigation, and reduces a foreign company's ability to contest a government demand for data access.").

[176] *Specification*, *supra* note 6 (The Specification, rather than the Cybersecurity Law, most resembles the better-known personal data security policy—the GDPR.); *see also* Sheng, *supra* note 165 ("This

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

sharing, transferring, and disclosing personal information in China.[177] The Specification has the potential to affect the already complex landscape of e-discovery in United States courts involving ESI stored in China.[178]

The Cybersecurity Law and the Specification work in tandem: the Cybersecurity Law outlines the broad laws, and the Specification details how to comply with them. The Specification is not a promulgated law but a regulation that provides guidance, which Chinese authorities have relied upon to determine compliance with the vague Cybersecurity Law.[179] The Specification provides guidance to data controllers[180] and compliance programs in China.[181] It further expands the definition of personal information to include information that reflects one's activities like browsing history in addition to identifying information.[182] In addition, the Specification requires data controllers to obtain explicit consent before they can collect a natural person's data.[183] The Specification also requires that data controllers retain personal data for the shortest period of time necessary, and the data controller must limit access to personal data to the minimum extent necessary.[184] Finally, under the Specification, data subjects have a right to have their data erased.[185]

---

specification is considered one of the most like the GDPR. While the Cybersecurity Law summarizes fundamental principles of personal information, the TC260 specification provides detailed guidance for compliance in information processing.").

[177] *Specification*, *supra* note 6; *see also* Sheng, *supra* note 165.

[178] *See generally* Hellewell & Mattei, *supra* note 8, at 30–32.

[179] Sheng, *supra* note 165.

[180] Luo & Bradley-Schmieg, *supra* note 167 (This standard applies to any public or private organization that has the power to decide the purpose and method of processing personal information.).

[181] *Id.*

[182] *Specification*, *supra* note 6, § 3.1 ("3.1 Personal Information 个人信息: All kinds of information, recorded by electronic or other means, that can be used, alone or combined with other information, to identify a specific natural person or reflect activities of a specific natural person."); *see also* Sara Xia, *China's Personal Information Security Specification: Get Ready for May 1*, CHINA LAW BLOG (Feb. 28, 2018), https://www.chinalawblog.com/2018/02/chinas-personal-information-security-specification-get-ready-for-may-1.html.

[183] *Specification*, *supra* note 6, § 3.1 ("3.6 Explicit Consent 明示同意: The explicit authorization by the PI [Personal Information [?]] subject of specific PI processing through a written statement or an affirmative action on the PI subject's own initiative."); *see also* Xia, *supra* note 182.

[184] Luo & Bradley-Schmieg, *supra* note 167.

[185] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

Evidence of enforcement of the new laws and regulation is scarce. There is some evidence that the Chinese government attempts to enforce the privacy laws when companies misuse data within its borders. In January 2019, the Chinese Ministry of Industry and Information Technology published a "blacklist" of data controllers who had "excessively collected sensitive personal data" in violation of data privacy laws.[186] Then, internet regulators announced plans to evaluate personal data acquisition practices of over one thousand mobile telephone application companies.[187] Regulators explained that mobile app companies with unsatisfactory compliance could potentially lose their business licenses.[188] No available evidence suggests that data controllers who have made a cross-border data disclosure pursuant to a foreign court order have been subjected to civil or criminal liabilities.

With passage of both the Cybersecurity legislation and Specification regulation, the Chinese government balanced contradictory policy concerns and, ultimately, provided greater privacy rights for the people in China from commercial surveillance while maintaining and enhancing the government's access to data.[189] The new data measures are representative of the uniquely Chinese dichotomous data privacy paradigm: the legislation and regulations build consumer trust in the digital economy "but does not undermine the government's ability to maintain control."[190] One such initiative has the broad, ambitious purpose of requiring all business entities operating in China to exclusively use hardware that simultaneously blocks access to data by unauthorized users and provides complete access to the Ministry of Public Security.[191] Chinese regulators continue to construct a uniquely Chinese[192] data privacy system through the promulgation of specifications and other types of regulatory programs.

---

[186] Sacks & Laskai, *supra* note 30.

[187] *Id.*

[188] *Id.*

[189] Louise Lucas, *China Emerges as Asia's Surprise Leader on Data Protection*, FIN. TIMES (May 30, 2018), https://www.ft.com/content/e07849b6-59b3-11e8-b8b2-d6ceb45fa9d0.

[190] Sacks & Laskai, *supra* note 30.

[191] Steve Dickinson, *China's New Cybersecurity System: There is NO Place to Hide*, CHINA L. BLOG (Oct. 7, 2019), https://www.chinalawblog.com/2019/10/chinas-new-cybersecurity-system-there-is-no-place-to-hide.html.

[192] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

Before the Specification, China's personal data privacy laws were patchwork and vague—not clearly defined and scattered throughout various statutes and regulations.[193] There is limited information evidencing how the new rules and regulations have impacted cross-border discovery; however, the limited evidence available suggests that the new legal privacy system in China has had little impact on cross-border discovery involving data stored in China and requested by litigants in U.S. courts.

B. The Data Privacy Overhaul's Effect on Cross-Border Discovery

Though a variety of scenarios have unfolded in discovery disputes following the data privacy overhaul in China, none has evidenced a change in the U.S. courts' analysis of cross-border discovery disputes.

For example, in *Brooks Sports v. Anta (China) Co.*, an American shoe company sued a Chinese-based company, Anta, for trademark infringement.[194] When Anta failed to produce documents pursuant to a discovery plan, *Brooks* moved to compel production of those documents under the FRCP.[195] In particular, Brooks requested relevant WeChat communications made by Anta directors.[196] The Anta directors refused to disclose the communications, citing protection under Chinese privacy laws.[197] Anta submitted an expert report detailing the Chinese privacy laws that protected the directors' WeChat communications.[198] The expert report made no mention of the Specification or the Cybersecurity Law; instead, it argued that the Chinese Constitution and other laws that predated the Cybersecurity Law protected the communications.[199] The expert did not mention the Cybersecurity Law despite its promulgation more than eighteen months prior to the filing of the motion to

[193] Daley et al., *supra* note 5, at 239.

[194] Brooks Sports, Inc. v. Anta (China) Co., No. 1:17-CV-1458 (LO/TCB), 2018 WL 7488924, at *1 (E.D. Va. Nov. 30, 2018).

[195] *Id.*

[196] *Id.* at *2.

[197] *Id.* at 10.

[198] Declaration of Jie Lin ¶¶ 6–12, *Brooks Sports*, 2018 WL 7488924 (No. 1:17-CV-1458 (LO/TCB).

[199] *Id.* at ¶¶ 7–8.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

compel. Unpersuaded, the court imposed sanctions on Anta, citing the refusal of the custodians of the WeChat communications to consent to their disclosure.[200]

In *3D Systems Corp. v. Miller*, plaintiffs requested that defendant Union Tech produce personal devices belonging to its employees under the FRCP.[201] The defendants argued that the Cybersecurity Law forbade the plaintiffs from transporting their devices outside of China.[202] They explained that without proper safeguards in the discovery protocol, making a cross-border transfer of the devices would violate the Cybersecurity law.[203] Nevertheless, the United States District Court for the Southern District of Indiana granted the plaintiff's motion to compel, reasoning "Union Tech's Chinese privacy law argument rings particularly hollow with regard to devices that have already been transferred out of China" and citing evidence that the custodians had the devices in their possession at a meeting in Chicago preceding the discovery dispute.[204]

The limited evidence available regarding the impact of the new data privacy system in China shows that little has changed when it comes to how litigants in possession of data stored in China respond to discovery requests and how courts analyze these disputes. In both *Brooks* and *3D Systems*, plaintiffs sought personal data stored on employee custodians' personal devices. In both cases, the defendants refused to produce the ESI, arguing that Chinese privacy laws protected the custodians' privacy interests. Although both disputes arose in 2018 following the promulgation of the Cybersecurity Law, only 3D Systems cited the Cybersecurity Law as blocking production of the data. The reliance on different laws to make the

---

[200] *Brooks Sports*, 2018 WL 7488924 at *18.

[201] 3D Sys. Corp. v. Miller, No. 1:17-cv-03252-RLY-MJD, 2018 WL 7350939, at *2 (S.D. Ind. Mar. 13, 2018).

[202] *Id.* In their response to 3D System's motion to compel, Union Tech laid out the necessary safeguards:

> [T]he Cybersecurity Law of the People's Republic of China, which came into effect June 1, 2017, imposes significant limitations on the transfer of electronic information outside of China. Persons who wish to transmit such data outside of China's borders must first obtain a security assessment based on review of that data. The Protocol does not provide any procedures for review of SEM devices in China or certification of the information on those devices prior to transfer to the U.S.

Union Tech, Inc.'s Response to Plaintiff's Motion to Compel the Forensic Analysis of Certain Electronic Devices ¶¶ 8-9, *3D Sys.*, 2018 WL 7350939 (No. 1:17-cv-03252-RLY-MJD).

[203] *3D Sys.*, 2018 WL 7350939, at *2.

[204] *Id.* at *2 n.3.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

same argument suggests that, although the Cybersecurity Law and Specification provide greater clarity concerning the data privacy laws in China and may be transformative in China itself, the new system may not necessarily block cross-border transfers coming out of China that were not arguably already blocked by the old system of data privacy regulations that were peppered throughout various laws.[205]

III. COURTS SHOULD NOT ALTER THE ANALYSIS OF DISCOVERY DISPUTES

Despite the shifting legal landscape in China and the changing ways entities must conduct business when dealing with data related to China, the new Cybersecurity Law and Specification should not change how U.S. courts resolve discovery disputes involving data stored in China. Courts will likely continue to compel parties in possession and control of ESI stored in China to produce the ESI under the FRCP. Because the goal of the U.S. pretrial discovery system is mutual knowledge of all relevant facts,[206] minimal change to the court's analysis is the right result.

Following the overhaul of the data privacy system in China, the Hague Convention likely continues to be an unreliable alternative to the FRCP when litigants in U.S. courts seek data stored in China. The Chinese Ministry of Justice has not reliably responded to letters of request issued under the Hague Evidence Convention,[207] and China has made restrictive reservations to the Convention.[208] No available evidence suggests that China has increased its efficiency in responding to letters of request, removed its reservations to the Hague Convention, or increased its willingness to assist U.S. courts in compelling production of documents that are blocked from cross-border production under China's privacy laws. Thus, U.S. courts should not increase the frequency with which they rely on Hague Convention procedures in discovery orders. Instead, courts should issue orders under the FRCP, analyzing the new Chinese data privacy laws as part of the new data privacy paradigm in China. While courts did not typically give much weight to laws protecting personal privacy rather than national interests, courts should view the

[205] *See* Daley et al., *supra* note 5, at 240.

[206] *See supra* note 1 and accompanying text.

[207] *See* Gucci Am., Inc., v. Weixing Li, No. 10 CIV. 4974(RJS), 2011 WL 6156936, at *9 (S.D.N.Y. Aug. 23, 2011), *vacated*, 768 F.3d 122 (2d Cir. 2014).

[208] Hague Convention, *supra* note 62.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

personal privacy protections as part of China's overall scheme to increase public confidence in the booming digital economy in China.[209] While courts should continue to ultimately weigh in favor of production under the FRCP, they should provide the entity or individual with possession of the data stored in China with protective measures, similar to how the Southern District of New York limited the discovery request in *Wultz* by requiring BOC to produce the documents to the court solely for an in camera review.[210] These protective measures will show that U.S. courts appropriately consider the personal data privacy laws as part of China's national interests, not just the personal interest of the individual whose data a litigant in a U.S. court requests.

Though some evidence has emerged that Chinese authorities have taken aggressive measures to enforce the Cybersecurity Law and Specification,[211] the enforcement will likely not influence the courts' analysis of the harm factor. Preceding the promulgation of the data security laws in China, courts were unlikely to weigh evidence of potential harm in favor of production under the Hague Convention, unless litigants pointed to harms experienced by similarly situated litigants in situations involving cross-border evidence disclosures.[212] As the currently available information evidences only enforcement of domestic compliance with the new data privacy laws, courts are unlikely to give additional weight to the harm factor. The hardship of compliance factor will likely not weigh in favor of production under the Hague Convention unless Chinese authorities begin subjecting entities who make cross-border data disclosures pursuant to litigation in foreign courts to civil or criminal liabilities.

Moreover, the new data privacy laws do not fundamentally alter the inverse relationship between the legal privacy paradigms that underlie the laws in U.S. and China. China's limited discovery process and protection of individuals' data from private entities has traditionally contrasted sharply with the inverse situation in the U.S. The U.S. has traditionally empowered its litigants to participate in the world's broadest pre-trial discovery process. And the U.S. has traditionally provided broad protections against the government while resisting regulation of how private entities may handle personal data. Even before the overhaul of its data privacy laws, China had a system of laws in place that limited litigants' ability to make a cross-border

[209] Sacks & Laskai, *supra* note 30.

[210] Wultz v. Bank of China Ltd., 942 F. Supp. 2d 452, 473 (S.D.N.Y. 2013).

[211] For failure to comply with data privacy laws, mobile app companies have faced blacklists and business license revocations. Sacks & Laskai, *supra* note 30.

[212] *See Gucci*, 2011 WL 6156936, at *34.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu

production of evidence in U.S. courts. The new laws increase the privacy rights of citizens within China and contain strict data localization regulations but are otherwise largely in line with older Chinese laws that blocked cross-border production of data.

IV. CONCLUSION

With the promulgation of increasingly strict data protection laws in China, U.S. litigants are likely to face challenges when seeking discovery of ESI stored in China. Despite the new laws, U.S. courts will likely still adhere to their commitment to broad discovery and will likely continue to order parties to produce ESI stored in China under the FRCP. Due to the lack of evidence of China's improved compliance with the Hague Convention and the lack of specific evidence that producing parties are facing new or harsher penalties under the new laws, courts should continue to compel production of discoverable ESI stored in China under the FRCP to fulfill the U.S.'s commitment to its open and reciprocal discovery system.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2020.777
http://lawreview.law.pitt.edu